

# Color Channel Characteristics (CCC) for Efficient Digital Image Forensics

Surbhi Gupta

Computer Science & Engineering Faculty  
I. K. Gujral Punjab Technical University  
Kapurthala, India  
royal\_surbhi@yahoo.com

Neeraj Mohan

Computer Science & Engineering Faculty  
I. K. Gujral Punjab Technical University  
Kapurthala, India  
erneerajmohan@gmail.com

**Abstract**-Digital image forgery has become extremely easy as low-cost image processing programs are readily available. Digital image forensics is a science of classifying images as authentic or manipulated. This paper aims at implementing a novel digital image forensics technique by exploiting an image's Color Channel Characteristics (CCC). The CCCs considered are the noise and edge characteristics of the image. Averaging, median, Gaussian and Wiener filters along with Sobel, Canny, Prewitt and Laplacian of Gaussian (LoG) edge detectors are applied to get the noise and texture features. A complete, no reference, blind classifier for image tamper detection has been proposed and implemented. The proposed CCC classifier can detect copy-move as well as image splicing accurately with lower dimensionality. Support Vector Machine is used for classification of images as authentic or tampered. Experimental results have shown that the proposed technique outperforms the existing ones and may serve as a complete tool for digital image forensics.

**Keywords**-image tampering; noise discrepancies; feature extraction; edge textural information; statistical evaluation

## I. INTRODUCTION

Wide digital image usage has led to their intended manipulation. Some manipulations can make the image more informative and useful. These manipulation types are called image enhancements. Other manipulations could change the content of the image altogether. Such manipulations are termed as image forgeries [1]. Image forgery is usually achieved using copy-move or image splicing operations [2-3]. When a subpart of an image is cropped, processed and then pasted into the original image the manipulation is called copy-move. When two or more images are required in order to build a new image it is called image splicing. Imaging forensic techniques are applied to distinguish and classify authentic and manipulated images. These techniques utilize the image data to locate whether the questioned image is authentic or manipulated. Some of these techniques try to define the origin of the image, whereas others try to compare it with some reference images. Some techniques extract features to check inconsistencies present in the image itself.

An image may be expressed using different color models like RGB, YCbCr, L\*a\*b etc. Each color model has three channels. The image intensity information is spread in these

three channels. The color information distribution among channels depends on the model used. In RGB Model, Red, Green and Blue channels contain equal amount of intensity information. But the human vision system cannot utilize RGB color for its apprehension. Luminance or brightness of color is the most important information which human vision system uses for understanding colors. Other models like L\*a\*b (Luminance, red minus green, green minus blue) and YCbCr (Luminance, chrominance blue, chrominance red) are based on Luminance. In these models, most of the intensity information is present in luminance channel. Another popular color model is HSV (Hue, Saturation and Value) model which is based on the human color perspective. It has hue, saturation and value channels for the distribution of intensity data. Different channels in these examples are capable to illustrate and bring out different features of an image. Color channel characteristics (CCC) for various models could be a genuine aid in image analyzing.

Various image forensic techniques have been proposed and analyzed in the last two decades. The author in [4] proposed a blind, noise based, passive image quality assessment model to transform the heuristics into noise structures. Mathematical models were developed to measure the edge sharpness, the random noise and the structural noise in an image objectively, without any reference image. Authors in [5] proposed Image Quality Measures (IQM) to expose compression and steganography using image statistical analysis. A linear regression classifier was used for image classification of original and manipulated images. Sequential floating forward search (SFFS) algorithm was applied for feature selection. The achieved accuracy was 91% and 80% for large and small manipulated regions of the image, respectively. Further, authors in [6] used noise variance of overlapping blocks to estimate manipulation in images, but this method did not execute well when images with high quality factors were spliced and resaved at a lower quality. Binary similarity measures (BSM) were introduced in [7]. BSM are based on correlation and texture features of the image. Feature selection was applied to attain an accuracy of 90% using joint feature sets. The major limitation of the approach was that its accuracy decreased when the image manipulated region was small. Authors in [8] proposed statistical noise feature extraction

using de-noising, wavelets and likelihood of neighbors. The classifier was 90% effective in classifying direct camera outputs from tampered versions. Authors in [9] proposed splice detection based on the measuring of statistical differences by using Discrete Cosine Transform (DCT) and image quality measures. Authors in [10] performed block-wise wavelet analysis followed by tiling sub-band HH1 and noise variance estimation for detecting manipulations. The main limitation of the algorithm was that it could not be used as an individual forgery detector and needed human intervention as well. Authors in [11] compared features from chroma and RGB channels for inserted objects' edge sensitivity and sharpness. But the outcomes were not illustrated for images at different quality factors. Authors in [12] used blocking, activity and zero crossing characteristics from YCbCr channels for locating the tampered area in manipulated images. Authors in [13] proposed the use of variance based noise estimation in forged images using principal component analysis (PCA) from hue, saturation and value channels with high accuracy. Recently, authors in [14] used Sobel operator to detect sharp-edged areas of foreign objects to localize the manipulated regions in the image efficiently. Other significant contributions used Natural Model [15], Markov Features [16], Gabor Filters [17], Multi-Scale Weber Local Descriptors [18] and Textural Features [19] for image forensics. These algorithms achieved high accuracy, but induced a big number of features and high computation time. Moreover, the execution of these techniques was not evaluated extensively for various JPEG images at different qualities. A forensic classifier for different quality JPEG images with high accuracy and low dimensionality is still required.

Literature study reveals that various color model channels have different data and hence different characteristics. These characteristics are named as color channel characteristics (CCC). This paper aims to propose CCC and further implement a CCC based image classifier with high accuracy and low computation time.

## II. CCC BASED FEATURE EXTRACTION

A forged image may be produced by copy-move, splicing or various other post processing operations. Only a robust technique can reveal such technical image forgeries. The proposed method uses statistical estimation of image noise and edge texture variation based on CCC. Every tampering operation leaves its traces on the image. These traces differentiate the tampered image from original one. The first and second order derivatives are obtained from different color channels to capture the discontinuities and highlight image tampering. The proposed feature set is extracted using RGB and YCbCr planes of the image. A CCC based classification Model is presented in Figure 1.

### A. Analysis of RGB Color Channel Characteristics for Feature Extraction

RGB image is also denoted as a true color image. For each pixel it gives the value of red, green, and blue color component. Hence, the intensity of the image element is obtained by combining the three color components at a particular pixel location. Useful information drawn for RGB channels could be

used for discriminating forged images from the original. Noise-based features could play a substantial role in differentiating direct camera images from their tampered version. One can elicit and analyze features from red, green and blue plane to highlight tampering. In the current study, statistical noise features from RGB channels are extracted and their use has been explored to differentiate tampered images from the original ones. The original image in most cases is not available, but it can be approximated by the use of a de-noising filter. The filter will get rid of the noisy sharp features of the available image. The filtered image will now be close to the original image. This de-noised image is compared with the tampered image to get the discontinuities. Authors in [8] extracted features using de-noising filtering and used them for detecting cropped regions in the image. Various de-noising filters, i.e. Averaging  $A(x, y)$ , Median  $M(x, y)$ , Gaussian  $G(x, y)$  and Wiener filters  $W(x, y)$  of  $3 \times 3$  size are considered for image forgery detection.  $A(x, y)$ ,  $M(x, y)$ ,  $G(x, y)$  and  $W(x, y)$  are defined as (1), (2), (3), and (4) respectively.

$$A(x, y) = \frac{1}{mn} \cdot \sum_{i=1}^m \sum_{j=1}^n F(x, y) \quad (1)$$

where  $F(x, y)$  represents the intensity at pixel location  $(x, y)$ .

$$M(x, y) = \text{median}\{F(x, y)\} \quad (2)$$

where  $(x, y) \in w$  and  $w$  represents a neighborhood defined by the user, centered on location  $x, y$  in the image. Gaussian low pass filter, with standard deviation 0.5, is explored for image forensics application in this work.

$$G(x, y) = \frac{1}{2\pi\sigma^2} \cdot e^{-(x^2+y^2)/2\sigma^2} \quad (3)$$

where  $x$  and  $y$  are the distances from the origin in the horizontal and vertical axis.  $\sigma$  is the standard deviation of the Gaussian distribution. Wiener filter filters the image to estimate the local image mean and standard deviation.

$$W(x, y) = \mu + \frac{\sigma^2 - v^2}{\sigma^2} \cdot (F(x, y) - \mu) \quad (4)$$

where  $\mu$  and  $\sigma^2$  estimate the local mean and variance around each pixel and  $v^2$  denotes noise variance. This study is based on the features extracted from R, G and B channels individually. The tampered image in every image channel, e.g. red, is filtered using de-noising filter and then the original red channel image is subtracted from the red filtered image. The absolute difference image is then analyzed. First order derivatives, i.e. mean and standard deviation are extracted as features using (5) and (6).

$$\mu = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N F(x, y) \quad (5)$$

$$\sigma = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N (F(x, y) - \mu)^2 \quad (6)$$

The algorithm used for noise based statistical feature extraction is presented below:

**Step 1:** Consider an image  $I$  and extract its RGB values.  $F_R(x, y)$ ,  $F_G(x, y)$  and  $F_B(x, y)$  represent the intensity values for red, green and blue planes respectively.

**Step 2:** Apply one of (1)-(4)  $3 \times 3$  filters, e.g. Gaussian filter, to obtain filtered image  $G(x, y)$ . Let  $G_R(x, y)$ ,  $G_G(x, y)$ ,  $G_B(x, y)$ ,

represent the Gaussian intensity value for red, green and blue planes respectively.

**Step 3:** Calculate the absolute difference  $D_R(x, y)$  between  $F_R(x, y)$  and  $G_R(x, y)$  by using (7):

$$D_R(x, y) = |F_R(x, y) - G_R(x, y)| \quad (7)$$

Then, compute the base-2 logarithm of  $D_R(x, y)$  using (8)

$$L_R(x, y) = \log_2(D_R(x, y)) \quad (8)$$

**Step 4:** Calculate mean and standard deviation as first order image derivatives using (5) and (6).

**Step 5:** Repeat step 3 and step 4 for Green and Blue channels to obtain  $3 \times 2 = 6$  features. Four different filters are used in the experiment, which means  $4 \times 6 = 24$  features.

Original and 10 tampered (T1-T10) images from MICC-F220 [20] database have been utilized for experimentation. Table I shows the results obtained for the mean and standard deviation for RGB channels and de-noising Median filter. Figure 2 shows the values obtained for mean and standard deviation features for median filter. Results indicate a clear difference in values obtained from original and tampered images. The value of the mean and standard deviation for all filters and all RGB planes is low as compared to its tampered versions. Figure 3 shows the scatter plots for mean and standard deviation features extracted from median filtering. A total of 12 features of the three R, G and B channels for four filters are calculated as mean and standard deviation features. It is evident from the scatter plots that value of features of original image differs significantly from the value of the features of tampered images while tampered images have similar values.

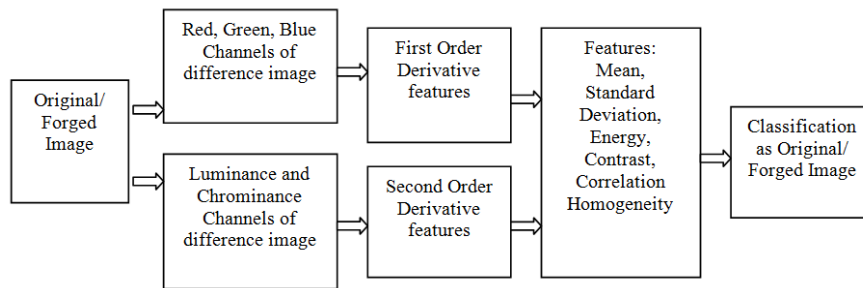
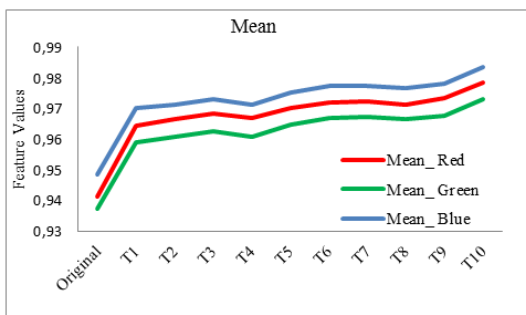
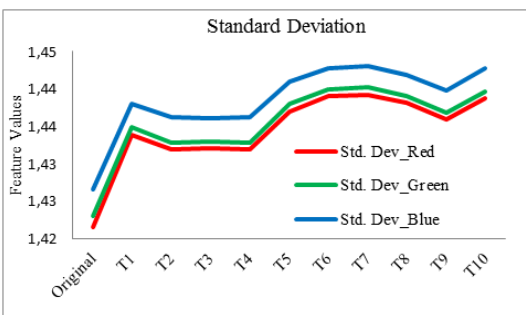


Fig. 1. CCC based model for image forensics



(a) Mean



(b) Standard Deviation

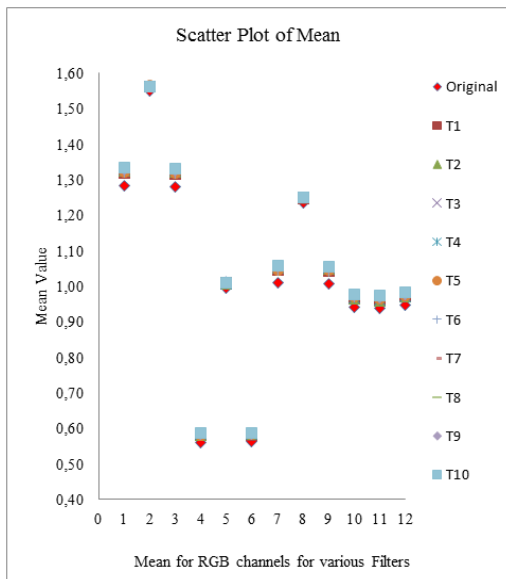
Fig. 2. Representation of mean and standard deviation feature extracted from median filtering

TABLE I. FEATURE EXTRACTION FROM MEDIAN FILTERING OF ORIGINAL AND TAMPERED IMAGES

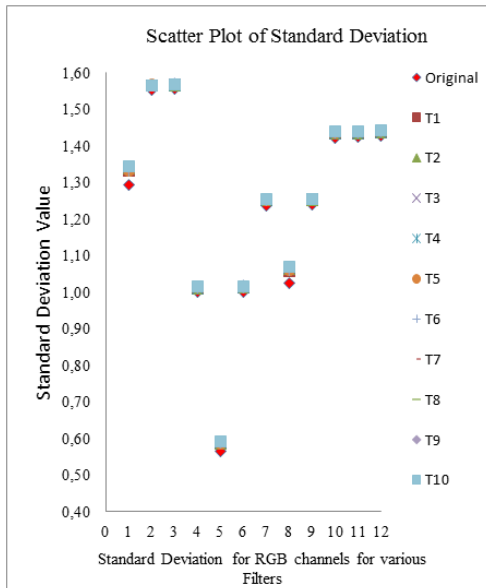
Image	Mean			Standard Deviation		
	Red	Green	Blue	Red	Green	Blue
Original	0.9414	0.9372	0.9486	1.4216	1.4229	1.4265
T1	0.9644	0.9591	0.9701	1.4338	1.4348	1.4380
T2	0.9667	0.9607	0.9713	1.4319	1.4328	1.4362
T3	0.9683	0.9626	0.9731	1.4321	1.4330	1.4360
T4	0.9667	0.9609	0.9714	1.4319	1.4328	1.4362
T5	0.9700	0.9648	0.9754	1.4370	1.4380	1.4409
T6	0.9719	0.9668	0.9773	1.4391	1.4400	1.4428
T7	0.9723	0.9671	0.9773	1.4393	1.4402	1.4431
T8	0.9711	0.9664	0.9766	1.4381	1.4391	1.4419
T9	0.9735	0.9678	0.9782	1.4358	1.4368	1.4397
T10	0.9785	0.9731	0.9836	1.4388	1.4397	1.4427

**B. Noise Feature Extraction from YCbCr Planes for Image Forensics**

Each color model has specific characteristics to indicate the image forgery. Most of the splice detection methods ignore the chroma component, but use the luminance component of the image to detect forgery. Nevertheless, image chroma (saturation) is very useful for color image splicing detection. In the YCbCr color model, Y represents the luminance component and Cb and Cr are the blue-difference and red-difference chroma components. Cb (or Cr) component has little image content while most of image content is preserved in Y component.



(a) Mean



(b) Standard Deviation

Fig. 3. Scatter plot for feature extracted from median filtering

As discovered in [11], the edge analysis in chroma channel is especially useful. Authors utilized chroma channels for extracting edge texture features from forged images. They demonstrated that chroma channels are specifically useful as they catch the crisp edges of spliced region. Gray level co-occurrence matrix (GLCM) for immediate neighbors was used to extract features. In present study, four edge detectors namely, Canny, Prewitt, Sobel and Laplacian of Gaussian have been explored for extracting features from Y, Cb and Cr channels. Figure 4 depicts the edge extraction using these different edge detectors. It is evident that edges of foreign objects, e.g. zebra in this image,

have sharper edges as compared to the edges of other natural objects present in the image.

The obtained images are used for extracting second order derivatives using GLCM. GLCM [22] is very useful in the study of pixel pair's relationship to examine image texture. It computes how many times a pair of intensity values occur in a particular neighborhood in an image. An example of GLCM extraction has been presented in Figure 5. An original image may contain many pixel pair relationships. All possible pixel pair relationships for image in Figure 5a are presented in Figure 5b. For each pair, the number of its occurrence is counted and listed in Figure 6c. For example, value '2' in the first cell of Figure 6c means that the pair (0,0) occurs twice in the example image.

Further, second order statistical features, i.e. for Energy, Correlation, Contrast and Homogeneity (ECCH) are extracted. Contrast measures the confined variations in the gray-level co-occurrence matrix. Correlation gives the joint probability occurrence of specific pixel pairs. Energy gives the sum of squared elements in the GLCM. Homogeneity denotes that how closely the factors in the GLCM are distributed to the GLCM diagonal.

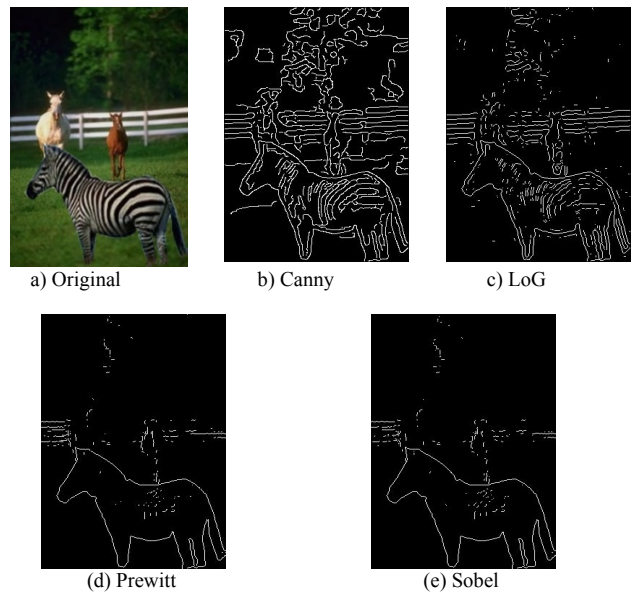


Fig. 4. Edge images obtained from dehrominance channel for different edges

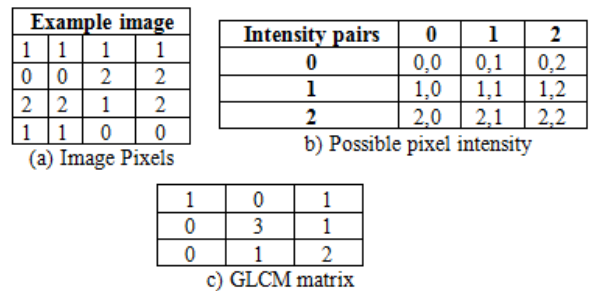


Fig. 5. Extracting GLCM matrix

TABLE II. EXAMPLE OF ECCH FEATURE EXTRACTION FROM CANNY EDGE OF ORIGINAL IMAGE AND ITS TAMPERED VERSIONS

	Energy			Correlation			Contrast			Homogeneity		
	Y	Cb	Cr	Y	Cb	Cr	Y	Cb	Cr	Y	Cb	Cr
Original	0.6991	0.7626	0.8331	0.4035	0.4371	0.4649	0.1176	0.0883	0.0594	0.9412	0.9558	0.9703
T1	0.7131	0.7953	0.8272	0.4161	0.4575	0.4675	0.1102	0.0739	0.0613	0.9449	0.963	0.9693
T2	0.7114	0.7951	0.8252	0.4158	0.4585	0.4696	0.111	0.0739	0.0619	0.9445	0.963	0.969
T3	0.7103	0.7935	0.8232	0.4172	0.4591	0.4716	0.1112	0.0744	0.0625	0.9444	0.9628	0.9688
T4	0.7104	0.794	0.825	0.4161	0.4583	0.4699	0.1113	0.0743	0.062	0.9443	0.9628	0.969
T5	0.7132	0.7964	0.8267	0.4145	0.4566	0.4673	0.1104	0.0736	0.0615	0.9448	0.9632	0.9692
T6	0.7126	0.7961	0.8272	0.4134	0.4557	0.4645	0.1108	0.0738	0.0616	0.9446	0.9631	0.9692
T7	0.7123	0.7967	0.8261	0.4124	0.4538	0.4633	0.1111	0.0737	0.0621	0.9445	0.9631	0.969
T8	0.7119	0.7964	0.8256	0.4121	0.4517	0.4624	0.1113	0.0741	0.0623	0.9444	0.963	0.9688
T9	0.711	0.7946	0.826	0.4144	0.4568	0.4684	0.1113	0.0742	0.0617	0.9443	0.9629	0.9691
T10	0.7097	0.7931	0.8246	0.4106	0.453	0.4634	0.1123	0.0751	0.0626	0.9438	0.9624	0.9687

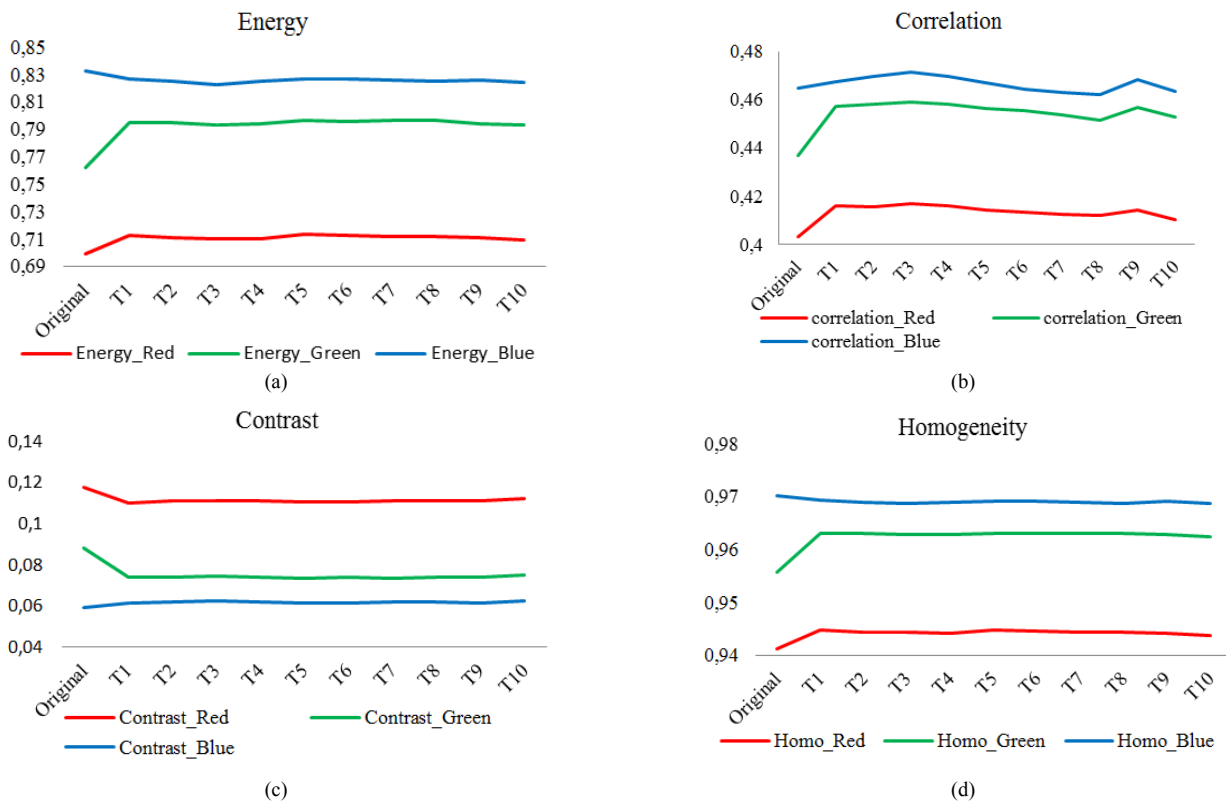


Fig. 6. Representation of a) Contrast, b) Energy, c) Correlation and d) Homogeneity feature extracted from median filtering

$$\text{Contrast: } \sum_i \sum_j (i - j)^2 c_{ij} \quad (9)$$

$$\text{Energy: } \sum_i \sum_j c^2_j \quad (10)$$

$$\text{Correlation: } \frac{\sum_i \sum_j (i^*j) * c_{ij} - \mu_i \mu_j}{\sigma_i \sigma_j} \quad (11)$$

$$\text{Homogeneity: } \sum_i \sum_j \frac{c_{ij}}{1 + |i - j|} \quad (12)$$

where  $i, j$  denotes a pixel pair. The algorithm used for texture based statistical feature extraction is:

**Step 1:** Consider an image  $I$  and extract its YCbCr channels.

$F_Y(x, y)$ ,  $F_{Cb}(x, y)$  and  $F_{Cr}(x, y)$  represent the intensity values for different channels.

**Step 2:** Apply edge detector to  $F_Y(x, y)$ , to obtain a binary edge image  $E_Y(x, y)$  and then obtain GLCM matrix for edge image  $P_Y(x, y)$ .

**Step 3:** Further, second order derivative features ECCH are calculated by using (9), (10), (11) and (12).

**Step 4:** Repeat Steps 2 and Step 3 for the other two channels to obtain  $4 \times 3 = 12$  features. Repeat algorithm steps 2 and 3 for another three edge operator to obtain  $12 \times 4 = 48$  features.

Table II indicates the results obtained from ECCH features for the canny edge operator. Features are extracted from Y, Cb and Cr channels of original and 10 tampered (T1-T10) images. Figure 6 demonstrates the values obtained for these features for original and tampered images. A clear deviation can be observed for the feature values of original and tampered images. Figure 7 shows the relevant scatter plots. It is evident that the value of the features of tampered images differs significantly from the value of the features of the original image. CCC based first and second order derivatives are used together for features extraction for classification of images. As shown above, a total of  $24+48=72$  features is extracted. The computational complexity of the algorithm is linear as every pixel is accessed only once.

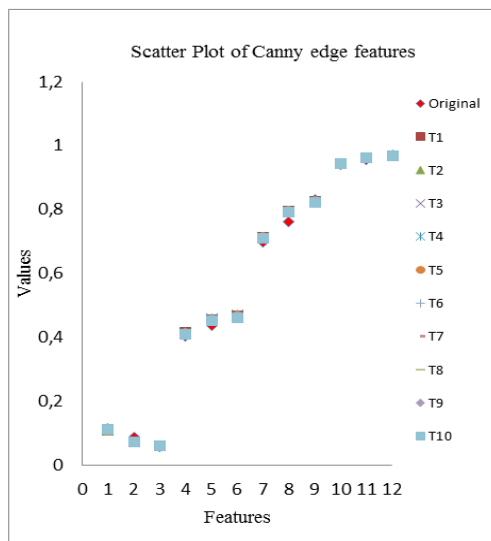


Fig. 7. Scatter plot for canny edge detector

### III. EXPERIMENTAL RESULTS

The experimental results of the proposed method have been obtained using a popular image dataset CASIA V2.0 [23]. This dataset consists of 7,491 authentic and 5,123 tampered images. Tampered images are produced using crop-paste and spliced image region(s). These images are pre-processed with resizing, rotation or other distortions. Images are post-treated with operations such as blurring to finish crop-and-paste operations. Different sizes (small, medium and large) of spliced regions have been studied. Experiment with 3 and 10 fold cross-validation approach has been conducted to assess the operation of the proposed method. Machine learning is achieved using support vector machines (SVM). SVM offer high accuracy and avoid over-fitting. SVM can perform comfortably even if data is not linearly separable in the base feature space. Kernel choice is crucial. The RBF Kernel of SVM gives the best results for binary classification. So, LIBSVM [24] classifier with radial basis function kernel is applied. The grid search method is used for choosing the penalty parameter C. All the experiments are tested on the mentioned dataset with LIBSVM classifier. The software platform used was Matlab R2012a. Hardware was a PC with 2.10 GHz Intel core 2 duo processor. The efficiency of the classifier is evaluated on the basis of

accuracy, feature dimensionality, feature selection and computation time. A classifier's accuracy is determined by the right image classifications. Dimensionality denotes the number of features used for the categorization. Lesser dimensionality means fewer features and less evaluation time. Feature selection is a technique used for the reduction of the number of used features. The non-contributing features may be ignored using feature selection procedure, but increases the evaluation time of the algorithm. The computation time is the time taken for feature computation and feature selection. The performance of the proposed method is investigated for different JPEG Compression Quality Factors as illustrated in Table III. The proposed classifier is further compared with existing state of the art classifiers. Accuracy, dimensionality and need for feature selection are compared and tabulated in Table IV. Comparison of computation time has been illustrated in Table V.

The main features of CCC classifier are:

- The classification accuracy of CCC classifier is better when authentic and forged images are of different quality. The classifier accuracy drops slightly when the spliced image is of high quality.
- CCC classifier's accuracy is superior compared to natural image model (NIM) [15], Markov features (MF) [16] and multi-scale WLD [18]. The comparison is illustrated in Figure 8.
- CCC classifier has low dimensionality. The accuracy of CCC classifier is similar to textural feature-based classifier [19] but with lower dimensionality.
- CCC classifier does not require feature selection. Classifier presented in [17] has a marginally higher accuracy compared to the proposed CCC classifier, but it additionally requires feature selection.
- CCC classifier computes the features of the complete image as a unit and does not involve image blocks for feature extraction. Moreover, feature selection is not commanded. This reduced the time as well as the space requirement for the proposed technique. Table V indicates that the computation time for CCC classifier is much lower compared to NIM [15] and MF [16] classifiers.

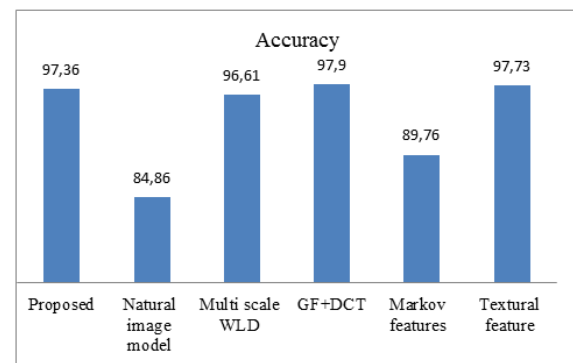


Fig. 8. Accuracy comparison of the proposed CCC classifier with existing classifiers



TABLE III. ACCURACY (%) AT VARIOUS JPEG QUALITY FACTORS

JPEG Image Quality Factor		Accuracy Obtained	
Authentic image quality factor	Spliced image quality factor	Accuracy (%) at 3-fold	Accuracy (%) at 10-fold
QF100	QF60	100	100
QF100	QF80	93.5	96.40
QF100	QF100	94.7	95.70
QF80	QF60	94.7	99.30
QF80	QF80	92.4	95.00
QF80	QF100	92.3	97.00
QF60	QF60	94.2	94.60
QF60	QF80	93.2	100
QF60	QF100	95.8	98.20
Average		94.53	97.36

TABLE IV. PERFORMANCE COMPARISON

Method	Accuracy (%)	Dimensionality	Feature selection
Proposed Method	97.36	72	Not Required
Natural Image Model [15]	84.86	266	Not Required
Markov Features [16]	89.76	100	Required
Multi Scale WLD [18]	96.61	960	Not Required
Textural Feature [19]	97.73	96	Not Required
GF+DCT [17]	97.9	70	Required

TABLE V. COMPUTATION TIME COMPARISON

Method	Feature Computation time(s)	Feature Selection time(s)	Total Computation time(s)
Proposed Method	1.4	-	1.4
Natural Image Model [15]	4.3	-	4.3
Markov Features [16]	2.2	2.1	4.3

#### IV. CONCLUSION

In this work, machine learning based blind JPEG classifier for detecting forged images using CCC based noise and edge characteristics is proposed and implemented. Statistical discriminating CCC features from original and tampered images are extracted. The original and spliced JPEG images at various quality factors are considered to train and test the classifier. The proposed classifier gives better efficiency in terms of higher accuracy and lower dimensionality. Moreover, its performance is high even for low quality JPEG images. The only limitation of CCC classifier is that the classification accuracy decreases slightly for high quality spliced image. The proposed classifier could be extended to detect copy move, seam carving, steganography and other types of image tampering and serve as a complete tool for image forensics.

#### REFERENCES

- [1] A. Rocha, W. Scheirer, T. Boult, S. Goldenstein, "Vision of the unseen: current trends and challenges in digital image and video forensics", *ACM Computer Survey*, Vol. 43, No. 4, pp. 26:1-42, 2011
- [2] H. Farid, "Detecting digital forgeries using bispectral analysis", Technical Report AIM-1657, AI Lab, Massachusetts Institute of Technology, 1999
- [3] G. K. Birajdar, V. H. Mankar, "Digital image forgery detection using passive techniques: A survey", *Digital Investigation*, Vol. 10, No. 3, pp. 226-245, 2013
- [4] X. Li, "Blind image quality assessment", *IEEE International Conference on Image Processing*, Vol. 1, pp. 1-449-1-452, 2002
- [5] I. Avcibas, S. Bayram, N. Memon, M. Ramkumar, B. Sankur, "A classifier design for detecting image manipulations", *International Conference on Image Processing*, pp. 2645-2648, 2004
- [6] C. Popescu, H. Farid, Exposing digital forgeries by detecting duplicated image regions, Technical Report TR2004-515, Dartmouth College, 2004
- [7] S. Bayram, I. Avcibas, B. Sankur, N. Memon, "Image manipulation detection", *Electron Imaging*, Vol. 15, No. 4, pp. 041102:1-17, 2006
- [8] H. Gou, A. Swaminathan, M. Wu, "Noise features for image tampering detection and steganalysis", *International Conference on Image Processing*, pp. 97-100, 2007
- [9] Z. Zhang, J. Kang, Y. Ren, "An effective algorithm of image splicing detection", *International Conference on Computer Science and Software Engineering*, pp. 1035-1039, 2008
- [10] B. Mahdian, S. Saic, "Using noise inconsistencies for blind image forensics", *Image and Vision Computing*, Vol. 27, No. 10, pp. 1497-1503, 2009
- [11] W. Wang, J. Dong, T. Tan, "Effective image splicing detection based on image chroma", *16th IEEE International Conference on Image Processing*, pp. 1257-1260, 2009
- [12] F. Battisti, M. Carli, A. Neri, "Image forgery detection by means of no-reference quality metrics", *IS&T/SPIE Electronic Imaging*, International Society for Optics and Photonics, pp. 83030K-83030K, 2012
- [13] Y. Ke, Q. Zhang, W. Min, S. Zhang, "Detecting Image Forgery Based on Noise Estimation", *International Journal of Multimedia and Ubiquitous Engineering*, Vol. 9, No. 1, pp. 325-336, 2014
- [14] B. Liu, C. M. Pun, "Splicing Forgery Exposure in Digital Image by Detecting Noise Discrepancies", *International Journal of Computer and Communication Engineering*, Vol. 4, No. 1, pp. 33-37, 2015
- [15] Y. Q. Shi, C. Chen, W. Chen, "A natural image model approach to splicing detection", *9th Workshop on Multimedia & Security*, pp. 51-62, 2007
- [16] Z. He, W. Lu, W. Sun, J. Huang, "Digital image splicing detection based on Markov features in DCT and DWT domain", *Pattern Recognition*, Vol. 45, No. 12, pp. 4292-4299, 2012
- [17] G. Muhammad, M. S. Dewan, M. Moniruzzaman, M. Hussain, M. N. Huda, "Image forgery detection using Gabor filters and DCT", *IEEE International Conference on Electrical Engineering and Information & Communication Technology*, pp. 1-5, 2014
- [18] M. Hussain, S. Qasem, G. Bebis, G. Muhammad, H. Aboalsamh, H. Mathkour, "Evaluation of image forgery detection using multi-scale Weber local descriptors", *International Journal on Artificial Intelligence Tools*, Vol. 24, No. 4, pp. 1540016-1540043, 2015
- [19] X. Shen, Z. Shi, H. Chen, "Splicing image forgery detection using textural features based on the grey level co-occurrence matrices", *IET Image Processing*, Vol. 11, No. 1, pp. 44-53, 2016
- [20] I. Amerini, L. Ballan, R. Caldelli, A. DelBimbo, G. Serra, "A SIFT-based forensic method for copy-move attack detection and transformation recovery", *IEEE Transactions on Information Forensics and Security*, Vol. 6, No. 3, pp. 1099-1110, 2011
- [21] J. Canny, "A computational approach to edge detection", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. PAMI-8, No. 6, pp. 679-698, 1986
- [22] R. M. Haralick, "Statistical and structural approaches to texture", *Proceedings of the IEEE*, Vol. 67, No. 5, pp. 786-804, 1979
- [23] J. Dong, W. Wang, "CASIA tampered image detection evaluation database", *IEEE China Summit & International Conference on Signal and Information Processing (ChinaSIP)*, July 6-10, 2013
- [24] C. Chang, C. J. Lin, "LIBSVM: a library for support vector machines", *ACM Transactions on Intelligent Systems and Technology*, Vol. 2, pp. 27:1-27, 2011