ISBN 978-93-84422-71-4
Proceedings of 2016 International Conference on Image Processing, Production and Computer Science (ICIPCS'2016)
London (UK), March 26-27, 2016 pp.92-96

Exploiting Color Model Characteristics for Highlighting Image Tampering

Surbhi Gupta[1], Parvinder Singh Sandhu[2]
[1] Research Scholar, I. K. Gujral Punjab Technical University, Jalandhar
[2] Research Guide, I. K. Gujral Punjab Technical University, Jalandhar

Abstract: *Because of advancement in information technology and image processing, Image Tampering and its forensics is gaining research interest. This paper aims at detecting image manipulations by exploiting the various color model characteristics. Each color models highlights certain specific properties of the image. So studying the various color models and extracting features from them may provide a clue to detect the presence of image manipulations. RGB, YCbCr and HSV color model based features such as mean and variance are extracted and then utilized for differentiating original image from manipulated one. SVM classifier is used for categorizing images. Experiments proved that features utilizing various color models together can detect the presence of manipulations.*

Index terms: *Image tampering, color models, feature extraction, noise inconsistency, quality metrics, statistical evaluation*

1. Introduction

The technology nowadays comes with its side effects. At one side we have information technology who is making our life and work simple. But at the other end it is misused by many. First researchers have to work on the implementation of a new technology and then to overcome its side effects and misuse. Like many other technologies, with the advancement in information technology and image processing software the manipulation of the images has also increased considerably from past few decades. Retouching of the images has been so prevalent that nowadays one can hardly believe their authenticity. Retouching may be done for enhancement purpose by keeping the contents of the image intact or for creating forged images by intentionally altering the contents. Moreover the availability of various free image processing software has made the scenario worst. Even an amateur can create forged images with ease.

Image forgery detection methods are broadly classified as active and passive methods. Active methods are preventive whereas passive methods are reactive. Active methods use precautionary measures to prevent forgery of images by using digital signatures or watermarks. One can check the authenticity of the document anytime by checking the watermark or signature present on it. It’s usually followed for official document and images to protect them from forgery. Usually a code is embedded in the image which can be checked later for ensuring its authenticity. But this method requires either hardware or software so it is not possible to use them for each and every image clicked. Such images are equally prone to forgeries and need special methods to detect the traces of manipulations. These types of methods come under passive methods. Such methods are adopted when an image not protected by active methods is suspected for forgery. Passive methods are further classified as [1]

- Source based detection
- Tampering operation based detecting
- Statistical irregularities based detection
- JPEG compression based detection

http://dx.doi.org/10.17758/UR.U0316025

2. Statistical Image Manipulation Detection Techniques Based on Color Channels

2.1. Manipulation Detection based on RGB:

Xin (2002) proposed blind image quality assessment without using reference images [2] using RGB channels. Proposed model works on edge sharpness level, the random noise level and the structural noise level. A mathematical tool is developed to transform the heuristics into noise structures under various circumstances. Later, Avcibas et al. (2004) conducted a statistical analysis of image quality measures which revealed different perspectives of image [3]. Author applied them to reveal compression and steganography. A linear regression classifier was then designed using the statistics collected. Then, Popescu and Farid in (2004) has given a method for detecting manipulation based on noise [4]. In this algorithm first the image is segmented into overlapping blocks and then the noise variance is estimated for each block. Lyu and Farid (2005) [5] in their paper extracted all the featured based on RGB color space from the image. A wavelet based image statistics is computed from RGB channels. Afterwards, Ng et al. (2005) [6] in their paper extracted a part of features using RGB channel. They demonstrated that statistics based on a joint color patch, fractal geometry and differential geometry in RGB color space can be used to differentiate the images. Bayram et al. (2006) validated the images based on three different forensic features based on Image quality metrics, multi-scale decompositions, correlation and texture properties [7]. The statistical tool named as Binary Similarity Measures (BSM) is introduced which is based on correlation and texture characteristics between the bit planes. Zhang et al. (2008) proposed a splice detection method based on multi-size block discrete cosine transform and image quality measures [8]. Their model measures statistical differences between original and fake image. Then Mahdian and Saic (2009) in their paper proposed an algorithm for detecting tampering using noise inconsistencies [9] by performing block wise analysis of wavelet, followed by tiling sub band HH1, followed by noise variance estimation. Gou et al. in his paper [10] (2009) performed feature extraction using RGB channels of the image. Difference aspects of noise based on de-noising algorithms, wavelet analysis and neighborhood prediction are used by the author. Noising aspects of the image are captures by extracting mean and standard deviation of pixel intensity from three channels. Further neighborhood prediction is performed to add more features. These features from RGB channel together with wavelet features are used for classification of original and tampered images. Classification of images is done using support vector machines and 90% accuracy is achieved. Recently Liu and Pun (2015) in [11] has developed an algorithm for detecting noise discrepancies. Their method segments the image based on objects and boundaries and then detect sharp edged areas using Sobel operator. Energy based graph cut is used to label the regions as manipulated area and original area.

2.2. Manipulation Detection based on YCbCr

Wang et al. (2009) proposed a feature extraction method based on chroma channel [12]. Author mentioned that edge sensitivity and sharpness of inserted objects is more visible in chroma channels of image rather than RGB channels. Paper demonstrated that in the edge images of Cb or Cr component spliced edges are not as smooth as the original image edges. Initially four edge images are created by considering immediate 4 neighbors in Cb image. Then Gray Level Co-occurrence matrix (GLCM) is used in the edge image of Cb component. Then features are extracted based on different threshold values. Accuracy of 64-89% is achieved for various thresholds and dimensions.

Later, Battisti et al. [13] (2012) has utilized blocking, Activity and Zero crossing characteristics from YCbCr channels to authenticate images and achieved good accuracy in localizing tampering. The proposed method used a combination of image quality degradation features.

2.3. Manipulation Detection based on HSV

Ianeva et al. (2003) [14] collected some features extracted from Hue, Saturation and Value. In this paper author proposed feature set constructed from HSV color space. Those features may also be used for steganalysis. These features are moments of characteristic function of wavelets sub-bands. Then, Chen et al (2007) [15] performed color image classification using HSV color space. However the author performed splice detection on only grayscale images. Features based on moments of characteristic function of wavelets sub-bands are again used for classification problem. Later, Ke et al. in (2014) performed the image classification based on variance in noise estimation using PCA from HSV image [16].

3. Statistical Noise Feature Extraction

In this section we will discuss the various parameters for feature extraction for evaluating forged images. These forged images may be a result of copy move, splicing or various other post processing operations. Our method is based on statistical estimation of image noise by extracting image features based on various color models. Every color model highlights different features of image. Depending on various color models we can extract much useful information which can be utilized to categorize original and fake images. The first sets of features are based on various de-noising models applied on RGB planes of the image. Second set of features are based on edge detection properties applied on YCbCr planes of the image. Third set of image features are extracted from HSV planes.

3.1. Feature Extraction from RGB planes

RGB image is also referred to as a "true color" image. It defines red, green, and blue color components for each individual pixel. The color of each pixel is determined by the combination of the red, green, and blue intensities stored in each color plane at the pixel's location. Useful information can be applied for discriminating forged images from original. Gou [10] in his paper has applied the denoising filter along with gaussian fitting error and neighborhood prediction based features. In this work we have applied de-noising algorithm to extract the image feature. Various noise filters are capable of capturing different aspects of the image. We have considered median and gaussian filter of size 3X3. Gaussian filter with standard deviation 0.5 is taken. First the RGB image is filtered using above mentioned filters and then subtracted from its original i.e. $I_{en}=I- I_f$

Where, I is original Image, I_f is filtered Image and I_{en} is estimated noise image.

Then the intensity range is expanded using log operation i.e. $I_l = \log_2 (I_{en})$

Then mean and standard deviation are taken as first set of features.

$$1^{st} \text{ feature: } \mu = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N} I_l \qquad (1)$$

$$2^{nd} \text{ feature: } \sigma = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(I_l - \mu)^2 \qquad (2)$$

Where M and N indicate the size of the image I.

Thus for every single plane we have 2X2=4 features and 3X4=12 features in total.

3.2. Features Extraction from YCbCr channels

Wang et al. [12] in their paper mentioned the utilization of chroma channels for extracting features from forged images. Author discussed that how Y, Cb, Cr channels are able to identify the sharpness of edged created due to copy move and splicing. They used GLCM with threshold for four edge images using four immediate neighbors to extract features. Further variation in threshold value is done to extract more features. In this work we have considered Sobel edge detector for extracting features from Y, Cb and Cr channels. Sobel edge detector is a gradient based method which works by using kernels to capture and highlight gradient changes in edges relative to the pixel grid.

I_{ed}=S (I), where, I is original image and I_{ed} is sobel applied image.

After applying edge detector GLCM matrices are created for each edge image to specify the pixel pair occurrences. We can utilize GLCM for different directions and offset to study more features if required. In this work we have considered right neighbor of the pixel only. Further energy and correlation are considered for each edge operator. Energy gives the sum of squared elements in the GLCM. Correlation measures the joint probability occurrence of the specified pixel pairs.

$$1^{st} \text{ feature: Energy} = \sum_{i=0}^{G-1}\sum_{j=0}^{G-1} P(i,j)^2 \qquad (3)$$

$$2^{nd} \text{ feature: Correlation} = \sum_{i=1}^{G-1}\sum_{j=0}^{G-1}\frac{\{i-j\} X\, P(i-j)-\{\mu_x-\mu_y\}}{\sigma_x X \sigma_y} \qquad (4)$$

Thus giving a total of 3X2=6 features for each image.

3.3. Feature Extraction from HSV planes

An analysis method based on the Hue-Saturation-Value (HSV) levels of an image can also be used for the classification of original images from forged ones. The Hue of a color is best described (by Sachs [17]) as the "tint". Saturation or "shade" is defined as the level of how pure or intense a color is. Value is the level of brightness (luminance) of a color or how light or dark it is. Intuitively, if an area or areas throughout an image are copied and pasted from different sources, the color and brightness, as captured from each respective camera, may be slightly different. Thorough analysis of HSV levels helps to determine this. Again mean and standard deviation are used as features from HSV planes.

4. Experimental Results

The proposed technique has been verified using jpeg image dataset. We have considered CoMoFoD[18] dataset. We have taken 600 images, 300 authentic and 300 spliced images from this dataset. All the images are in JPEG format. The manipulated set of images consists of copy move with pre-processing techniques used. Moreover the size of forged area considered is also varying. We used Support Vector Machine which is a widely used efficient classifier for such applications. For image classification we used LIBSVM [19] with RBF kernel. Grid searching is used to select parameters. We used 70% original and 70% manipulated images for training and the remaining ones for testing. We observed good performance for most of the manipulations. We computed the fraction of correctly classified manipulated images (P_D) and wrongly classified as manipulated images (P_F). The P_F obtained is close to 83% and P_D is close to 7%. This suggests that the methodology is quite able to identify the original images from manipulated ones. Although human intervention can always boost the results.

5. Conclusion

Passive or blind techniques and methodologies for validating the integrity and authenticity of digital images is one of the rapidly growing areas of research. Passive methods require no extra prior knowledge of the image content or any embedded watermarks or signature. This paper presented a technique which utilizes the information from various color models to statistically differentiate tampered image from original. All features are extracted from RGB, YCbCr and HSV color models. SVM classifier is used to classify images and good true positive ratio is obtained. Results obtained shows the efficiency of methodology used. Utilizing more color models and features may enhance the suitability of the presented methodology.

6. References

[1] G. K. Birajdar and V. H. Mankar, "Digital image forgery detection using passive techniques: A survey", *Digital Investigation*, 2013, *10*(3), 226-245.
http://dx.doi.org/10.1016/j.diin.2013.04.007

[2] Li. Xin, "Blind image quality assessment", *Proceedings of International Conference on Image Processing*, 2002, Vol. 1. IEEE.
http://dx.doi.org/10.1109/ICIP.2002.1038057

[3] I. Avcibas, S. Bayram, N. Memon, M. Ramkumar, B. Sankur, "A classifier design for detecting image manipulations", *Proc. International conference on image processing (ICIP)*, 2004. p. 2645–8.

[4] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions", *Technical Report TR 2004-515,* Department of Computer Science, Dartmouth College, 2004.

[5] S. Lyu and H. Farid, "How realistic is photorealistic?" *IEEE Transactions on Signal Processing,* 53, pp. 845-850, February 2005.

[6] T.-T. Ng, S.-F. Chang, J. Hsu, L. Xie, and M.-P. Tsui, "Physics-motivated features for distinguishing photographic images and computer graphics*," in ACM Multimedia*, Singapore, November 2005.

[7] S. Bayram, I. Avcibas, B. Sankur and N. Memon, "Image manipulation detection ", *Electron Imaging,* 2006;15(4). 041102-1–041102-17.
http://dx.doi.org/10.1117/1.2401138

[8] Z. Zhang, J. Kang, Y. Ren, "An effective algorithm of image splicing detection", *Proc. International conference on computer science and software engineering*, 2008. p. 1035–9.
http://dx.doi.org/10.1109/csse.2008.1621

[9] B. Mahdian and S. Saic, “Using noise inconsistencies for blind image forensics”. *Image and Vision Computing,* 2009, *27*(10), 1497-1503.
http://dx.doi.org/10.1016/j.imavis.2009.02.001

[10] H. Gou, A. Swaminathan, M. Wu, “Noise features for image tampering detection and steganalysis”, *Proc. International conference on image processing* (ICIP) 2007. p. 97–100.
http://dx.doi.org/10.1109/icip.2007.4379530

[11] B. Liu and C. M. Pun, “Splicing Forgery Exposure in Digital Image by Detecting Noise Discrepancies”, 2015, *International Journal of Computer and Communication Engineering*, *4*(1), 33.
http://dx.doi.org/10.7763/IJCCE.2015.V4.378

[12] W. Wang, J. Dong and T. Tan, “Effective image splicing detection based on image chroma”. *Image Processing (ICIP), 2009,* 16th IEEE International Conference on (pp. 1257-1260). IEEE.
http://dx.doi.org/10.1109/icip.2009.5413549

[13] F. Battisti, M. Carli and A. Neri, “Image forgery detection by means of no-reference quality metrics”. *IS&T/SPIE Electronic Imaging,* 2012, pp. 83030K-83030K, International Society for Optics and Photonics.

[14] T. Ianeva, A. de Vries, and H. Rohrig “Detecting cartoons: a case study in automatic video-genre classification,” in *IEEE International Conference on Multimedia and Expro*, 1, pp. 449- 452, 2003.
http://dx.doi.org/10.1109/icme.2003.1220951

[15] W. Chen, Y.Q. Shi, and G. Xuan, “Identifying computer graphics using hsv color model and statistical moments of characteristic functions,” in *2007 IEEE International Conference on Multimedia and Expo*, July 2007, pp. 1123–1126.
http://dx.doi.org/10.1109/ICME.2007.4284852

[16] Y. Ke, Q. Zhang, W. Min and S. Zhang, “Detecting Image Forgery Based on Noise Estimation”, 2014, *International Journal of Multimedia and Ubiquitous Engineering*, *9*(1), 325-336.
http://dx.doi.org/10.14257/ijmue.2014.9.1.30

[17] J. Sachs, *Digital Image Basics*. Digital Light & Color. 1999

[18] D. Tralic, I. Zupancic, S. Grgic and M. Grgic, "CoMoFoD - New Database for Copy-Move Forgery Detection", *in Proc. 55th International Symposium ELMAR-2013*, pp. 49-54, September 2013.

[19] C. C. Chang and C. J. Lin, “LIBSVM: a library for support vector machines”, *ACM Transactions on Intelligent Systems and Technology*, 2:27:1--27:27, 2011.