Identification of Digital Image Using Illumination Color Classification

Tawhare Poonam K., Thorat Radhika G., Khoje Puja N., Kanade Amrut.V.

Abstract— Forgery detection is the most important task in our national judicial system and criminal investigation procedure. Today digital images have become powerful source of communication. With the advancement of technology, it becomes very easy to change the content of digital images. Due to which these images are no more taken as a proof of authenticity or legitimacy. In our system, we deal with the widely used form of image tampering known as image composition or image splicing. We demonstrate an effective algorithm to detect the spliced images based on illumination inconsistencies present in images. We propose a forgery detection method that exploits subtle inconsistencies in the color of the illumination of images. Our approach is machine-learning based and requires minimal user interaction. The technique is applicable to images containing two or more people and requires no expert interaction for the tampering decision. From these illuminant estimates, we extract texture and edge-based features which are then provided to a machine-learning approach for automatic decision-making. A support vector machine (SVM) is used to classify the given images as either genuine or forged.

Index Terms— Forgery Detection, Support Vector Machine (SVM), Representation Learning, Facial Features.

I. Introduction

A. Image Forgery And Detection

Images have become a powerful tool for communication nowadays as they are used every day in newspapers, magazines, websites and advertisements and provide various information. As the use of images are increasing day by day but trust in images is decreasing day by day. Creating a fake image from original image is known as Image forgery and to check whether the image is original or fake is probably termed as Image forgery Detection. Moreover, digitally manipulated images can trigger off major controversies. Hence, there is a need for more sophisticated and mathematically sound techniques that can perform this task of classification of the image into real ones and digitally manipulated ones. Digital image processing is the use of computer algorithms to perform image processing on digital images. As a subcategory or field of digital signal processing, digital image processing has many advantages over analog image processing. It allows a much wider range of algorithms to be applied to the input data and can avoid problems such as the build-up of noise and signal distortion during processing. Since images are defined over two dimensions (perhaps more) digital image processing may be modelled in the form of multidimensional systems.

Nowadays, millions of digital documents are produced by a variety of devices and distributed by newspapers, magazines, websites and television. In all these information channels, images are a powerful tool for communication. Unfortunately, it is not difficult to use computer graphics and image processing techniques to manipulate images. However, before thinking of taking appropriate actions upon a questionable image, one must be able to detect that an image has been altered. Image composition (or splicing) is one of the most common image manipulation operations when assessing the authenticity of an image, forensic investigators use all available sources of tampering evidence. Among other telltale signs, illumination inconsistencies are potentially effective for splicing detection: from the viewpoint of a manipulator, proper adjustment of the illumination conditions is hard to achieve when creating a composite image. Thus illuminant color estimates from local image regions are analyzed and illumination map is obtained as a result. As it turns out, this decision is, in practice, often challenging. Moreover, relying on visual assessment can be misleading, as the human visual system is quite inept at judging illumination environments in pictures. Thus, it is preferable to transfer the tampering decision to an objective algorithm. In this work, an important step towards minimizing user interaction for an illuminant-based tampering decision-making is achieved. Hence a new semiautomatic method that is also significantly more reliable than earlier approaches is proposed. Quantitative evaluation shows that the method achieves a detection rate higher than the previous approaches. We exploit the fact that local illuminant estimates are most discriminative when comparing objects of the same (or similar) material. Thus, we focus on the automated comparison of human skin, and more specifically faces, to classify the illumination on a pair of faces as either consistent or inconsistent. User interaction is limited to marking bounding boxes around the faces in an image under investigation. In the simplest case, this reduces to specifying two corners (upper left and lower right) of a bounding box.

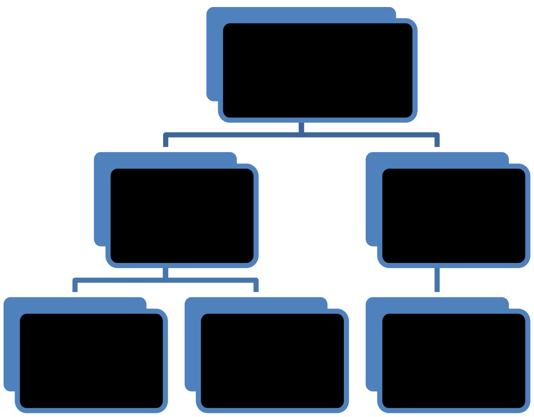
B. Image Forgery Approaches

There are basically two approaches of digital image forgery detection-

A. Active Approach:

Data hiding: In this approach, it adds secondary data into an image. Digital watermarking is a common example of this. In this, digital watermark is inserted at source side and verify that at detection side. The main drawback of this method is that watermark must be inserted at the time of recording, which requires specially equipped digital camera.

Digital signature: In this approach, unique feature of image is extracted and corresponding signature created at the source side. This signature is then used for verification at the detection side.



B. Passive Approach:

This approach does not need any prior information about image like it does not need any digital signature generated or watermark embedded in advance. This is the main advantage of passive methods. This techniques work on the assumption that although digital forgeries may leave no visual clues that indicate tampering, they may alter the underlying statistics of an image. Detecting the changes in statistical properties and is known as digital image forensics.

I. Objectives

1. To propose a forgery detection method that exploits subtle inconsistencies.
2. By using minimum amount of human interaction provides a crisp statement on the authenticity of the image.
3. Provide security for safety.

II. Literature Review

In this section we are present the different methods those are for digital image forgeries detection with their advantage and problem.

H. R. Chennamma [8], Lalitha Rangarajan, Portions of the image is correlated with each other with respect to the imaging device. Such correlations will be disturbed in spliced images. We have used an intrinsic camera parameter, namely lens radial distortion, for the detection of image splicing. Inconsistency in the degree of lens radial distortion across the image is the main evidence for the detection of spliced images. In this paper we propose a novel passive technique (with no watermark or signature) for detecting copy-paste forgery by quantitatively measuring lens radial distortion from different portions of the image using line-based calibration.

Zhenhua Qu, Guoping Qiu, and Jiwu Huang [9] described a completely automatic method for detecting igital image splicing forgeries base on the sharp splicing boundaries. The novelty of the proposed method that an OSF based edge sharpness measure, a visual saliency guided feature extraction method and also a hierarchical classifier used to splicing detection problem. They explain that a trustworthy hierarchical classifier can be trained with the discriminative features extracted from the first few fixations predicted with a visual attention model with edge sharpness as visual cues and localizing splicing boundaries A drawback of this is that the edge sharpness cues now used will fail when concealing measures, such as blur, is useful.

Johnson and Farid[10] proposed spliced image detection by exploiting specular highlights in the eyes . In a subsequent extension, Saboia et al. automatically classified these images by extracting additional features, such as the viewer position. The applicability of both approaches, however, is somewhat limited by the fact that people's eyes must be visible and available in high resolution.

Y. Ostrovsky, P. Cavanagh, and P. Sinha, authors in [7] find that once the geometrical regularity of the previous displays is removed, the visual system is remarkably insensitive to illumination inconsistencies, both in experimental stimuli and in altered images of real scenes. Whether the target is interpreted as oddly illuminated or oddly pigmented, it is very difficult to find if the only cue is deviation from the regularity of illumination or reflectance. Our results allow us to draw inferences about how the visual system encodes illumination distributions across scenes. Specifically, they suggest that the visual system does not verify the global consistency of locally derived estimates of illumination direction.

Tiago Carvalho, Christian Riessy Elli et al. [1], proposed method for detecting forged images of people that exploit light inconsistencies in the color of the illumination of images. This method is machine learning-based and requires minimal user interaction. The method is valid to a broad range of images and requires no expert interaction for the tampering decision (provides crisp statement on authenticity of an image). To get this, they include hint (cue) from physics as well as statistical-based illuminant estimators on image regions of comparable material. From these illuminant estimates they mine (extract) texture- and edge-based features feeding a machine learning approach for automatic decision-making. They used support vector machine to classify these features. This method requires images of people with minimum two faces and prefers semiautomatic method for face extraction.

III. Problem Statement

The main aim of the project is to propose a forgery detection method that exploits subtle inconsistencies. Our approach is machine learning based and requires minimal user interaction. No expert interaction for the tampering decision, the technique is applicable to images containing two or more people. On image regions of similar material, to achieve this we incorporate information from physics and statistical based illuminant estimators. We extract texture and edge based features which are then provided to a machine learning approach for automatic decision making. The classification performance using an SVM meta-fusion classifier is promising. It yields detection rates of 86% on a new benchmark dataset consisting of 200 images, and83% on 50 images that were collected from the Internet.

IV. Proposed Work

We make an important step towards minimizing user interaction for an illuminant-based tampering decision-making. We propose a forgery detection method that exploits subtle inconsistencies in the color of the illumination of images. Interpretation of the illumination distribution as object texture for feature computation. Our approach is machine-learning-based and requires minimal user interaction.

The technique is applicable to images containing two or more people and requires no expert interaction for the tampering decision. To achieve this, we incorporate information from physics- and statistical-based illuminant estimators on image regions of similar material. From these illuminant estimates, we extract texture and edge-based features which are then provided to a machine-learning approach for automatic decision-making.

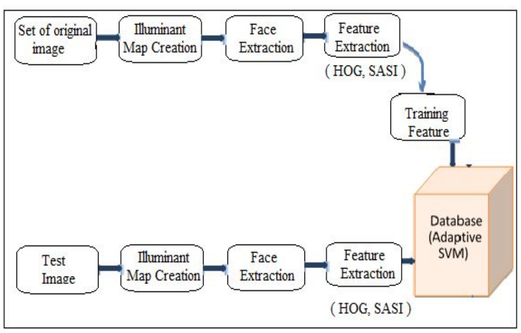


Fig 1. System Flow

V. Methodology

The method is broadly classified into five components:

A. Dense Local Illuminant Estimation

The input image is segmented into a specific type of regions, which are the regions of similar constant hue, by using algorithm. For each such regions mentioned above, illuminant color of the regions is calculated. The generalized grey world estimates is one color estimator and an estimate based on physics which is called as inverse-intensity chromaticity space estimator are used for obtaining the illumination estimates. The two illuminant maps are obtained by recoloring the regions with similar hue. The both illuminant maps obtained are then examined individually afterwards.

a) Generalized Gray World Estimates:

The gray world which is based on the assumption that the mean color of an image or picture is gray. If there is variation or deflection of the mean of the image intensities from the presumed gray color results because of the illuminance .Author extended this scheme of gray world hypothesis by inclusion of three parameters which are Derivative order (n): the assumption that the mean of the illuminants is gray can be extended to the absolute value of the sum of the derivatives of the image. Minkowski norm (p): Rather than summing-up image intensities, better results can be achieved by computing the path Minkowski norm. In Gaussian smoothing preprocessing the image is don so as to remove noise and smoothen the image.

b) Inverse Intensity-Chromaticity Estimates:

In this approach, the image intensities which obtained are assumed to show a combination of diffuse and specular reflectance. Diffuse reflection is the reflection of light from a surface such that an incident ray is reflected at many angles .Specular reflection is the mirror-like reflection of light, in which light ray coming from solitary direction is reflected into solitary outgoing direction. In the voting procedure, two conditions are enforced on a small region to increase flexibility with induced noises. If a small region does not fulfill the conditions stated above, then such small regions are de-categorized from voting procedure. The final estimate of the illuminant is based on majority votes of the obtained estimates.

B. Face Extraction

It is needed that all the faces in an image or photograph that are needed for consideration should be enclosed with the bounding boxes .The bounding boxes can be procured by using an automated algorithm or a human operator is chosen for bounding boxes. The advantages using a human operator for bounding boxes are that a human is better at judging the area of face to be enclosed in bounding boxes, reduces missed faces as well as false detection of faces another reason for preferring human over automated algorithm is the scene context is crucial in determining the lighting situation. Given a scenario there is an image where all persons under consideration are illuminated by the single source of light. The illuminants are expected to be similar. On the contrary, assuming that a person in the foreground is illuminated by camera flashlight and a person in the background is illuminated by surroundings light. There will be dissimilarity in the color of the illuminants is presumed. This small dissimilarity are difficult to figure out in a fully automated technique, but this can be eliminated with the human intervention.

C. Computation of Illuminant Features

a. Texture Description:

The SASI Statistical Analysis of Structural Information descriptor which is used for obtaining information regarding the image from illuminant maps. The salient aspect of using this descriptor is its ability to detect discontinuities in patterns of texture and capture minute granular information. Dissimilar illuminant colors interact varying with the surfaces differing in types, which gives dissimilar illumination. This descriptor estimates structural attributes of textures, which is uses the information from autocorrelation of horizontal, vertical and diagonal pixel lines at different scales. Another autocorrelation is calculated on the basis of specific fixed orientation, scale, and shift. The mean and standard deviation of all pixel values gives two feature aspects. This process is repeated for calculating different orientations, scales and shifts and applied till it gives a 128-dimensional feature vector. In the last step the obtained feature vector normalization is done.

b. Interpretation of Illuminant Edges

Extraction of Edge Points: The Canny edge detector used for obtaining edge points from the illuminant map of the face region, which gives edge points that are close in distance to each other. The number of edge point obtained may be large for minimizing the number of edge points; an approach is applied on the output of the Canny edge detector. A starting point is selected as a seed point, all other edge pixels in a region of interest which are centered around the seed point are then discarded from the process. The edge points nearer to region of interest are elected as seed points for the next step. This operation is repeated on the whole image till number of points are minimized and it is assured that every face region has similar or approximate density of points.

Point Description: The Histograms of Oriented Gradients is computed which gives description about the distribution of the chosen edge points. This Histograms of Oriented Gradients uses the concept of normalized local histograms as a basis for obtaining image gradient orientations. The HOG descriptor is built neighboring every edge points. The area around of this type of an edge point is called as cell. Each cell gives localized 1-D histogram of quantized gradient directions. The feature vector for this obtained feature descriptor is created by combining the histograms of all cells which are distributed in spatially larger region, of which histogram contrast is normalized. The output of this Histograms of Oriented Gradients is used as feature vector for the next steps.

c) Visual Vocabulary:

The number HOG vectors that are obtained differs, which is contingent upon the size and structure of the face which is being analyzed. The visual dictionaries are created to get feature vectors of specified length. This Visual dictionaries form a powerful representation, in which every face is assumed as a group of region descriptors. The spatial location of each of this region is eliminated. The visual dictionary is built by subdividing the data given for training into feature vectors of original and altered images. Every group is then clustered into clusters by applying the k-means algorithm .After applying k-means a visual dictionary is built using the visual words, where every word is characterized by the center of the cluster. By this, the most representative feature vectors of the training set are epitomized by the visual dictionary.

d) Quantization Using the Precomputed Visual Dictionary:

The HOG feature vectors obtained are then mapped to the visual dictionary. Every feature vector in an image is characterized by the nearest word in the dictionary which is the distance of Euclidean norm. A histogram is obtained for the word counts in the dictionary which in turn represents the distribution of HOG feature vectors in a face of the image.

D. Paired Faces:

The same descriptors for each of the two faces are merged for analyzing and comparing the two faces. The SASI-descriptors obtained on gray world can be coupled together for similarity .The scheme behind this is a feature concatenation from two faces is distinct when one of the faces is an original and another is doctored one. The Statistical Analysis of Structural Information descriptor and Histograms of Oriented Gradients edge descriptors seize two varying attributes of the face regions. The both descriptors can be imagined are digital signatures with distinct operations in digital signal processing context. The average value and standard deviation for each feature dimension is calculated. The feature dimensions with the max difference in the average values for are considered.

E. Classification:

The illumination for every pair of faces in an photograph or image can be categorized as consistent or inconsistent. By supposing that all chosen faces are illuminated by the same lighting conditions, the image labeled as doctored if a pair is categorized as inconsistent, the discrete feature vectors are categorized by utilizing support vector machine classifier which makes use of radial basis function kernel. The SASI feature and HOG edge features impart information that are supportive of each other .A technique based on machine learning is used for improving the detection performance. Every combination of illuminant map and feature type are separately classified by making use of 2class SVM classifier to for getting the distance between the image's feature vectors and the classifier decision boundary. The marginal distances provided by all individual classifiers to build a new feature vectors are combined by SVM-Meta Fusion.

VI. Algorithm Implementation

Algorithm1: Histograms of Oriented Gradients (HOG)

Histogram of Oriented Gradients (HOG) is a very powerful feature extractor used in the area of image processing. It generally focuses on detecting the shape of structures present in images. For this purpose, it tries to capture the gradient information from these images. The implementation of HOG algorithm is given below:

Step 1: The first step is to partition the image into small cells usually of size 8x8 pixels.

Step 2: Each pixel present in the cell corresponds to gradient orientation bin. Also there are fixed number of gradient orientation bins in each cell. Separate each cell into angular bins according to gradient orientation.

Step 3: Calculate the weighted gradient from these angular bins.

Step 4: The next step is to combine these cells in order to form a block which is usually of size 4x4 cells.

Step 5: Normalize the histogram in accordance with their energy over blocks. The set of normalized histogram represent the block histogram and these blocks represent the feature descriptor.

HOG is very popular and widely used because of its ability to remain constant to various photometric and geometric changes.

Algorithm2: SASI: Statistical Analysis of Structural Information

Statistical Analysis of Structural Information (SASI) given by Yarman-Vural and Carkacioglu is used to extract texture information from illuminant maps. SASI is more advantageous because of its capability to identify the similar textures.

The general algorithm of SASI given by Yarman-Vural and Carkacioglu is as follows:

Step 1: Select the neighborhood system, where d is the order of neighborhood system.

Step 2: The next step is to choose the sizes S of clique window.

2.1 Calculate the lag vector v (k. l) used for each clique window.

Step 3: For each clique window W

3.1 For each lag vector v (k.l)

3.1.1 For each pixel

3.1.1.1 Define clique window W

3.1.1.2 Calculate r(k,l)

3.2 Calculate mean value and standard deviation of r(k,l)

Step 4: Construct vector and normalized vectorer.

VII. CONCLUSION AND FUTURE WORK

The authenticity of an image is major research challenge in the field image forensic for real world events. The image integrity verification as well as identifying the areas of tampering on images without need to any expert support or manual process or prior knowledge original image contents is now days becoming the challenging research problem. Thus to solve this problem recently some more techniques were presented and new techniques will be developed to make better and harder to detect fakes (for exposing photographic frauds). In this paper we have discussed different methods of detection for digital image forgery as well as illumination inconsistencies and illuminant map. For the future work we suggest to work over improved new method with efficient skin detection methods.

ACKNOWLEDGMENT

Authors thanks to project guide Prof. Kanade A. V. who always being with presence & constant, constructive criticism to made this paper. We would also like to thank all the staff of COMPUTER DEPARTMENT for their valuable guidance, suggestion and support through the project work, who has given co-operation for the project with personal attention. Above all we express our deepest gratitude to all of them for their kind-hearted support which helped us a lot during project work. At the last we thankful to our friends, colleagues for the inspirational help provided to us through a project work.

REFERENCES

[1] Tiago José de Carvalho, Student Member, IEEE, Christian Riess, Associate Member, IEEE, Elli Angelopoulou, Member, IEEE, Hélio Pedrini, Member, IEEE, and Anderson de Rezende Rocha, Member, IEEE, "Exposing Digital

[2] Image Forgeries by Illumination Color Classification", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 7, JULY 2013

[3] C. Riess and E. Angelopoulou, "Scene illumination as an indicator of image manipulation," Inf. Hiding, vol. 6387, pp. 66–80, 2010.

[4] Yeung MM, "Digital watermarking", ACM Communications 1998; 41(7):30–3.

[5] Rey C, Dugelay JL. "A survey of watermarking algorithms for image authentication", EURASIP Journal on Applied Signal Processing; 2002: 613–21.

[6] Zhang C, Cheng LL, Qiu Z, Cheng LM, "Multipurpose watermarking based on multiscale curvelet transform", IEEE Transactions on Information Forensics and Security December 2008; 3(4):611–9.

[7] Farid H,"Image forgery detection – a survey", IEEE Signal Processing Magazine March 2009; 5:16–25.

[8] Y. Ostrovsky, P. Cavanagh, and P. Sinha, "Perceiving illumination inconsistencies in scenes," Perception, vol. 34, no. 11, pp. 1301–1314, 2005.

[9] H. R. Chennamma, Lalitha Rangarajan "Image Splicing Detection Using Inherent Lens Radial Distortion" IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 6, November 2010.pp 149-158.

[10] Zhenhua Qu, Guoping Qiu, and Jiwu Huang," Detect Digital Image Splicing with Visual Cues", LNCS 5806, pp. 247–261, 2009

[11] M. Johnson and H. Farid, "Exposing digital forgeries through specular highlights on the eye," in Proc. Int.Workshop on Inform. Hiding, 2007, pp. 311–325

[12] R. Tan, K. Nishino, and K. Ikeuchi, "Color constancy through inverse-intensity chromaticity space," J. Opt. Soc. Amer. A, vol. 21, pp. 321–334, 2004.

[13] J. van de Weijer, T. Gevers, and A. Gijsenij, "Edge-based color constancy," IEEE Trans. Image Process., vol. 16, no. 9, pp. 2207–2214, Sep. 2007.