ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 6, Special Issue 5, March 2017

National Conference on Advanced Computing, Communication and Electrical Systems - (NCACCES'17)

24th - 25th March 2017

Organized by

C. H. Mohammed Koya
KMEA Engineering College, Kerala- 683561, India

Behaviour Knowledge Space-Based Fusion for Image Forgery Detection

Navya Sara Monson[1], Manoj Kumar K.V.[2]

M. Tech Student, Department of Computer Science and Engineering, GEC Thrissur, India[1]

Professor, Department of Computer Science and Engineering, GEC Thrissur, India[2]

ABSTRACT: The detection of manipulated images is of utmost significance nowadays, mainly due to the various technological, moral, and judicial connotations associated with image editing. In this paper, a common form of image manipulation known as image composition or splicing is examined. The forgery detection method proposed here makes use of fine inconsistencies in the colour of the lighting of images. Our approach is machine-learning based which makes use of a behaviour knowledge space. This technique can be used in photographs having two or more people. To achieve forgery detection, complementary illuminant estimators are incorporated on image regions of similar material. Colour-, texture- and edge-based features are extracted from these illuminant estimates which are then provided to a machine-learning approach for automatic decision-making.

KEYWORDS: Image forensics, machine learning, spliced image detection, texture and edge descriptors.

I. INTRODUCTION

Images are one of the most shared forms of digital information these days and hence are a powerful tool for mass communication. Miscreants who understood the role of the ubiquitous nature of images in influencing public opinion have taken to manipulating images to take business or personal advantage. In this context, the research community has placed large importance on detecting manipulated images and curb the ramifications these images have on the society.

Image splicing or composition is one of the most common image tampering operations. In image splicing a new image is constructed by combining parts of two or more images. There have been many instances where people have used image splicing for their own benefit. There are several legal and ethical issues related to image tampering and the addressal of these issues can be done only after successful identification of altered images.

The forgery process leaves behind different evidences indicative of manipulation of which inconsistencies in compression or in the association of neighbouring pixels can be examined image features. Among different tampering evidences left behind by image composition, lighting inconsistencies are potentially effective in composition detection. Irregularities in the lighting of an image have enthused researchers because it is very hard to create a digital composite image that has a perfect illumination adjustment. Instead of using explicit physical properties of light which includes the direction of light, one can modify images into a different representation space to highlight vestiges of the forgery process. In this vein, we recommend the use illuminant maps (IM) as an alternate space to emphasize inconsistencies in forged images.

In our approach, we analyse colour, texture and shape features in an image to check for inconsistencies. The image to be checked is converted to more than one illuminant map. Inconsistencies, if any, become more pronounced in an illuminant map. This paper focuses on the automated analysis of human skin, and especially faces, to classify the illumination on a pair of faces as either consistent or inconsistent. We make use of the fact that local illuminant estimates are more discerning when items of similar material are compared. In this work, we examine attributes and features of an image that best describe it to better find out cues to detect a fake image.

The text is organized into three more sections. Section II provides brief descriptions of some of the most current methods in the literature that use illuminant information for detecting of composite images. Section III elaborates on the proposed method which uses the Behaviour-Knowledge Space method as the machine learning technique. Section IV gives conclusions and scope of future advancements.

II. LITERATURE SURVEY

Image tampering is widespread these days with the availability of low-priced computing gadgets and strong photo editing softwares. With a suitable photo editing tool (e.g., Adobe Photoshop or Pixlr) anyone can fabricate plausible photomontages easily. Over time the quality of image editing software has grown which has led to a higher level of credible images and difficulty of detection. This leads to the need of equally powerful forgery detection software for detecting fake images.

Methods for detecting image splicing by examining illumination inconsistencies is roughly split into two types: (a) the ones that check for mismatches in the setting of the light source; and (b) those that check discordant light source colours from the photo. The second group of approaches focuses on approximating scene illuminants and studying their different characteristics.

Gholap and Bora [1] initiated the use of illuminant colours to recognize composite images. Their work is based on the dichromatic reflection model presented by Tominaga and Wandell [2]. This method requires the presence of distinct specular highlight regions and assumes a single light source that illuminates a scene.

An augmentation to the Inverse-Intensity Chromaticity Space, initially proposed by Tan et al. [5] is used by Riess and Angelopoulou [3] , to estimate illuminant colour by segmenting the image into different parts and for finding out inconsistencies. Unlike the method used by Gholap and Bora, which considers whole objects for illuminant estimation, Riess and Angelopoulou's technique, takes small parts of objects for illuminant estimation and hence is more robust. A drawback of this method is that it is reliant on the human user to a certain extent during the segmentation of objects and the visual interpretation of the results. Also in cases where an image is subject to successive compressions and decompressions the transformed representation will not be visually suggestive of the presence or not of a forgery.

de Carvalho et al. [4] introduced a technique that builds upon Riess and Angelopoulou [3] and intents to lessen user dependency. This method is specifically useful for doubtful images consisting of humans.The authors estimate illuminant maps for the photo by means of complementary approaches. Texture and shape based features are extracted to characterize faces in the image. Finally classification of the image as real or fake is carried out by machine learning techniques such as SVM.

Carvalho et al. [6] addresses a drawback in de Carvalho et al. [4] – automated identification of the forged part in an image labelled as fake. It also assesses complementary information present in illuminant maps. This paper derives most of its procedural order from this paper.

In the next section, we elaborate a process which attempts to identify fake images and the face that is forged automatically using the Behaviour Knowledge Space method.

III. METHOD

This section describes the image forgery detection methodology, step by step.

A. OVERVIEW OF FORGERY DETECTION

Existing forgery detection methods rely on a human expert's verdict and prior knowledge. With the advent of technology, more efficient image editing tools create spliced images that make forgery detection a time consuming process. Moreover, the composite images created these days are difficult to detect with a visual analysis.

The proposed method aims to classify input images into one of two pre-defined class (real or fake) to detect forged images. A classification model is devised to categorize incoming images to one of the classes. The approach is to detect forgeries involving people by minimizing user interaction.

The image forgery detection methodology contains four main steps:

1. **Description:** this step creates the illuminant maps (an alternate illustration space of the input image), extracts image features (e.g., texture, color and shape), and transforms features into feature vectors;
2. **Classification:** the feature vectors created in the previous step are used by algorithms to learn image patterns to effectively classify the images.
3. **Labelling:** knowledge acquired from the image descriptors and the classification model is used in labelling a new image.

4. **Forgery Localisation:** after detecting a fake image, this step deals with finding out which face in the image is most likely to be forged. Figure 1 shows the module-wise segregation of the method where each module will be elaborated in the following sections.

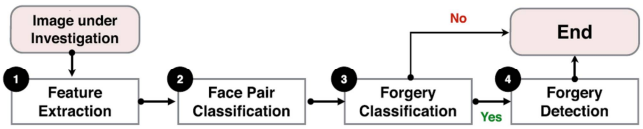

Fig.1: Forgery Detection Methodology

B. *DESCRIPTION*

The description phase of the methodology has 4 steps: a) representation of the image as an IM, b) face extraction, c) feature extraction from IMs and d) pairing of face features.

a) Representation of the image as an IM: There are two main classes of colour constancy algorithms: statistics-based and physics-based. Colour constancy algorithms are used for illuminant estimation by creating an Illuminant Map (IM) of the input image. Hypotheses formulated based on the statistics of image pixels are the foundation of statistics-based IM estimation algorithms and physics-based IM estimation methods are based on postulatory conceptualisations of the interaction between light and objects. The generalized grayworld estimates (GGE) serves our purpose of representing our image in a space that captures statistics-based information.

Physics-based information is captured using an extended version of the inverse-intensity chromaticity space (IIC) proposed by Riess and Angelopoulou [3].

b) Face Extraction: A bounding box is drawn by the user for each face to extract all the faces in the image. The bounding box can be specified by providing the coordinates of the upper left and lower right corners of each face.

c) Feature Extraction From IMs: In this step we extract visual properties or features (e.g., texture, shape, colour, among others) for analysis to find cues of splicing in the image. Texture is an important feature to be considered because light behaves similarly when incident on surfaces of the same texture. Since our focus is on faces and light incident on human skin is comparable due to similar reflective properties we consider texture as one of the features for learning purposes. In contrast with texture properties, shape properties of Illuminant Maps of forged faces differ from the shape properties of Illuminant Maps of faces initially in the image. This characteristic can also be made use by the learning process to distinguish between fake and real faces. Shape techniques used in our method make use of shape alignments and associations between adjacent shapes. These characteristics are useful for splicing because in fake images neighbouring shapes in regions of composed faces show very low correlation. Colour is also an important feature to be observed since we are dealing with light and its inconsistencies. This assigns importance to the colour of the light and hence colour is another important visual descriptor that has to be encoded while constructing feature vectors.

C. *CLASSIFICATION*

We aim to implement a classifier fusion technique called the Behavior – Knowledge Space. The most appropriate classifiers for the task need to be identified and selected. These classifiers should be combined for an improved performance compared to that of a single classifier. Faria *et al.* [7] has proposed a classifier selection and fusion framework that can be used in this context.

Initially, a set of classifiers are trained on the images of a training dataset. The outcome of each classifier on another set of images called the validation set is stored in a matrix. The information stored in this matrix is used to select a set of classifiers that when combined exhibit higher performance. Five diversity measures are calculated to get the extent of agreement between all classifiers used initially. At the end, a few classifiers are selected based on the above measures. These classifiers form a good mix for our classifier fusion technique.

We use the Behaviour-Knowledge Space method [8] as our classifier fusion technique. Many classifier fusion techniques assume that the classifiers in the classifier fusion are independent. But in reality this is not the case. If there is no a-priori knowledge about the behaviours of individual classifiers, then it is safer to treat each classifier on an equal basis. However when a-priori information about the individual classifiers' behaviour exists, we can derive knowledge which specifies the different quality of classifiers' behaviour so that better combination methods can be explored. The BKS is a good knowledge model that can fully represent and well organize knowledge extracted from former behaviour of classifiers as well as support convenient manipulation of contained knowledge.

A behaviour-knowledge space (BKS) is a K- dimensional space where each dimension corresponds to the decision of one classifier and has decision values equal to the number of decisions plus one. At the junction of the decisions of classifiers resides one unit of the BKS.; in each unit the method accumulates the number of incoming samples for each

class. Each unit of the BKS contains three kinds of data: (1) the total number of incoming samples, (2) the best representative class and (3) the number of incoming samples belonging to each class.

D. LABELLING

An image containing *q* people will have nC_q face-pairs. The classification of any paired feature as fake will lead to the classification of the image as fake Otherwise, the image is classified as a real image.

E. FORGERY LOCALISATION

The next step in the process is to point out the area in a fake image which has been manipulated. To localize the area where forgery may have been performed we make use of the information from the different IMs constructed. IMs created using different principles will have different aspects for the same image. This is because of the difference in principles used. It has been noticed that the IMs of fake faces differ more in colour appearance compared to the IMs of real faces. This difference in IMs can be used to locate the area of forgery.

IV.CONCLUSION

Manipulating public opinion by means of forged images involving people is a common malpractice these days. The circulation of such images in social media for forging particular impressions on a particular situation or person is widespread. No matter what the consequences of image editing are, it is necessary to construct suitable solutions to identify such ventures. The quality of the editing process has gone up with modern image editing softwares. Recently, questionable images involving politicians, movies stars and child pornography have raised several issues.

Even though technology provides different solutions to the problem at hand, many solutions in the literature depend on the knowledge of experts and information about the scene. This paper focuses on reducing user interaction by an automated decision making system. The system analyses and extracts aspects of an image that defines the image. These aspects are studied and made use in the decision making process.

In this work, an image is represented in a transformed space called the illuminant map. An illuminant map highlights the lighting used for illuminating the scene in the image so that lighting inconsistencies in the image can be used for finding out discrepancies. Image descriptors that study texture, shape and color cues are used to scrutinize the aspects that help in identifying forgeries. The color descriptors are analysed to check if similar objects are lighted by the same light. The relevance of texture descriptors comes from the fact that objects of the same type have similar texture and same reflective properties. Object borders and shape related properties are captured by shape cues.

Further, we proceed to use the Behaviour-Knowledge Space method as the classifier fusion technique for efficient classification. After classifying an image, we proceed to point out the area of forgery.

REFERENCES

[1] S. Gholap and P. K. Bora, "Illuminant colour based image forensics,"in Proc. IEEE Region 10 Conf., Nov. 2008, pp. 1–5.
[2] S. Tominaga and B. A. Wandell, "Standard surface-reflectance model and illuminant estimation," J. Opt. Soc. Amer. A, vol. 6, no. 4, pp. 576–584, Apr. 1989.
[3] C. Riess and E. Angelopoulou, "Scene illumination as an indicator of image manipulation," in Proc. Inf. Hiding Workshop, vol. 6387. 2010, pp. 66–80.
[4] T. J. de Carvalho, C. Riess, E. Angelopoulou, H. Pedrini, and A. Rocha, "Exposing digital image forgeries by illumination color classification," IEEE Trans. Inf. Forensics Security, vol. 8, no. 7, pp. 1182–1194
[5] R. T. Tan, K. Nishino, and K. Ikeuchi, "Color constancy through inverse intensity chromaticity space," J. Opt. Soc. Amer. A, vol. 21, no. 3,pp. 321–334, 2004.
[6] Tiago Carvalho, Fábio A. Faria, Hélio Pedrini, Ricardo da S. Torres, and Anderson Rocha," Illuminant-Based Transformed Spaces for Image Forensics", IEEE Transactions On Information Forensics And Security, Vol. 11, No. 4, April 2016
[7] F.A.Faria, J.A. dos Santos,A. Rocha, and R. da Silva Torres, "A framework for selection and fusion of pattern classifiersin multi-media recognition", Pattern Recognit. Lett., vol. 39, no. 4, pp. 52–64, Apr. 2014.
[8] Y. S. Huang and C. Y. Suen, "A method of combining multiple experts for the recognition of unconstrained handwritten numerals," IEEE Trans. Pattern Anal. Mach. Intell., vol. 17, no. 1, pp. 90–94, Jan. 1995