International Journal of Control Theory and Applications

ISSN : 0974-5572

© **International Science Press**

Volume 10 • Number 30 • 2017

Illumination Map Based Image Splicing Detection

P. Malarvezhi[a] M.S. Prashanth[b] RR.Abineash[b] G. Harish Iyer[b] T. S. Subashini[c] C. Dinadhayalan[d] and D.Vaishnavi[d]

[a] *Assistant Professor, Department of ECE, SRM University, kattankulathur*
[b] *Department of ECE, SRM University, kattankulathur*
[c] *Associate Professor, Department of Computer Science and Engg., Annamalai University*
[d] *Department of Computer Science and Engg., Annamalai University*

Abstract: One of the most common image tampering operations is splicing or composition. It consists in using parts of two or more different images to construct a new image depicting a moment that never happened in space and time. It is not difficult to find cases in which people use image composition to take business or personal self-advantage. In this project work transformed spaces, represented by image illuminant maps are explored, to propose a methodology for selecting complementary forms of characterizing visual properties for an effective and automated detection of image splicing forgeries. Statistical telltales provided by different image descriptors that explore color, shape, and texture features are combined to detect forgeries. This work focuses on detecting image forgeries containing people and present a method for locating the forgery, specifically, the face of a person in an image.

Keywords: *Image tampers detection, Image Splicing, Illumination map, SVM, SURF.*

1. INTRODUCTION

Today images are regarded as a notable communication media in our digital world and it is appear as the most shared documents at social networks, mainly because current mobile devices allow anyone to capture thousands of images anywhere at any time. In this scenario, the evolution of methods for make sure image authenticity is neededin modern society [1], [2]. This test might be a quietthat checking whether an image has been reworked for enhancement purposes (*e.g*., brightness or contrast) or as complex as revealing if the image has been tampered.

Image splicing or composition is most usual tampering operations. It is carried out by pasting the parts of more than one images to create a new image to give a picture that never occur in space and time. It is not difficult to find cases in which people use image composition to take business or personal self- advantage. Consider the following two cases.In May 2013, the conman Dimitri de Angelis was sentenced to twelve years in prison for deceiving investors using "photoshoped" photos in which he appeared alongside many different prominent people as, for example, former US president Bill Clinton, as Fig. 1.(*a*) portrays.In November 23rd 2012, a fake photo went viral in the Internet purporting Brazil's former president Luiz Inácio Lula da Silva beside Rosemary de Noronha, a suspicious gang leader investigated by the Brazilian Federal Police (Fig. 1.(*b*)).

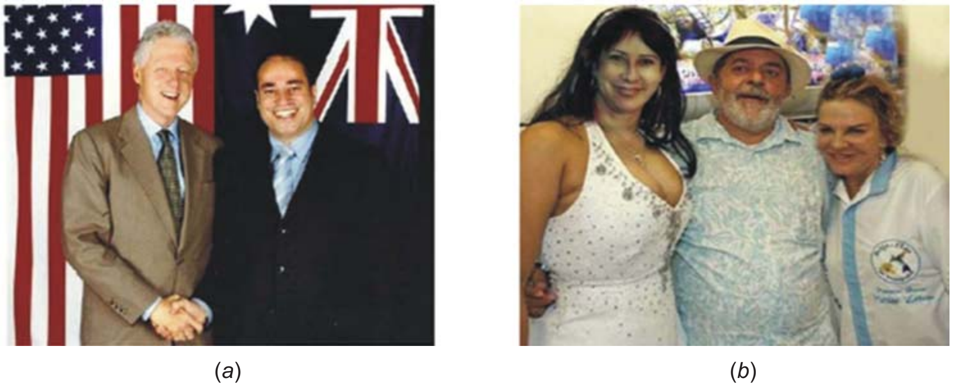


Figure 1: Fake images created through splicing. (*a*) Conman Dimitri de Angelis (right) alongside US former president Bill Clinton (left). (*b*) Fake image of Brazil's former president (center) in a purported personal life moment with an investigated gang leader

During the image authenticity verification, the 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. These composite images can be explored by capturing the artifacts and pin point in image transform spaces. For example, the authors in [3], given input videos as visual rhythms of Fourier Spectra for emphasizing artifacts related to biometric spoofing in face recognition system. Hence, this work uses the illuminant maps (IM) [4] as a transformed representation space to emphasis diverse kinds of irregularities exist in fake images.

In this work, inconsistencies of color, texture and shape present in a fake image become more pronounced in the transformed image, which is obtained converting an input image to different illuminant maps. More specifically, this work extends upon the method recently proposed by de Carvalho et al. [1], in which the authors use texture and edge descriptors to characterize IMs and detect inconsistencies in images pointing out possible tampering operations. In this work, usage of different color spaces and appropriate image descriptors and classifiers to better capture visual properties that might lead to forgery detection was carried out. The paper is organized as follows: Section 2 describes some of the most recent methods in the literature that consider, in different levels, illuminant information for detection of image splicing. Section 3 introduces the proposed methodology and its details and Section 4 gives the implementation details and results and finally, Section V presents conclusions and future work.

2. RELATED WORKS

The digital age, with all its facilities, also has its nuisances. One of them, empowered by cheap computing devices and powerful image editing software, is photo tampering. With little effort and a proper image manipulation tool (*e.g*., Adobe Photoshop or Gimp), ordinary people can create masterpieces depicting unbelievably credible photomontages with ease. In addition, the ever-growing quality and power of image editing software have taken image splicing to a whole new level of credibility and difficulty of detection. There are vast numbers of works proposed in literature to detect the fake images[5-9]. Among them, illumination based approaches are significant methods, which involves estimating the light source position or reconstructing a full illumination model from the scene.

Gholap and Bora [10] have used the dichromatic reflection model proposed by Tominaga and Wandell [11], which assumes a single light source to estimate illuminant colors from images. Dichromatic planes are estimated through Principal Component Analysis (PCA) from each specular highlight region of an image. Applying a Singular Value Decomposition (SVD) on an RGB matrix extracted from highlighted regions, the authors extract the eigenvectors associated with two significant eigenvalues to construct the dichromatic plane. This plane is then mapped onto a straight line, named *dichromatic line*, in normalized rg-chromaticity space. For distinct objects illuminated by the same light source, the intersection point produced by their dichromatic line intersection represents the illuminant color. Francis *et al.* [12] have also used the dichromatic reflection model to estimate illuminant colors in human skin highlighted regions. Based on chromaticity coordinates of the estimated illuminant color, the authors quantify the amount of chromaticity from each person in the image and use it to detect forgeries by matching distributions obtained from people in the same image.

Wu and Fang [13] have proposed a new way to detect forgeries using illuminant colors. Their method divides a color image into overlapping blocks estimating the illuminant color for each block. The authors used the algorithms Gray-World, Gray-Shadow, and Gray-Edge [14] to estimate the illuminant color. In addition, they used a maximum likelihood classifier proposed by Gijsenij and Gevers [15] to select the most appropriate method for representing the illuminant of each block. For forgery detection, the authors choose some blocks as reference and estimate their illuminants. The angular error between reference blocks and a suspicious block is calculated. If this distance exceeds a threshold, a block is classified as manipulated. This method is also strongly dependent on user interaction and perception to choose correct reference blocks. If the reference blocks are incorrectly chosen, for example, the performance of the method is strongly compromised.Carvalho*et al.* [1] have proposed a different way to use illuminants for detecting forgeries. In a custom-tailored method for detecting image compositions involving people, the authors estimate illuminant maps for the image using statistics-based and physics based approaches. Texture and shape descriptors are used to characterize these illuminant maps on face regions. The forgery detection is then performed through machine learning techniques such as SVM classifiers.

3. PROPOSED METHODOLOGY

This section describes each step of the proposed image forgery detection methodology. The splicing detection process commonly relies on the expert's experience and background knowledge. This process usually is time consuming and error prone as image splicing are even more sophisticated, and visual analysis may not be enough to detect forgeries. The proposed splicing detection task consists in labeling a new image among two pre-defined classes (real and fake) and later pointing out the face with higher probability to be the fake face. In this process, a classification model is created to indicate the class to which a new image belongs. The proposed image forgery detection methodology comprises five main steps as followings.

1. **Illuminant Estimation (IE) :** The input image is segmented into homogeneous regions. Per illuminant estimator, a new image is created where each region is colored with the extracted illuminant color. This resulting intermediate representation is called illuminant map (IM).

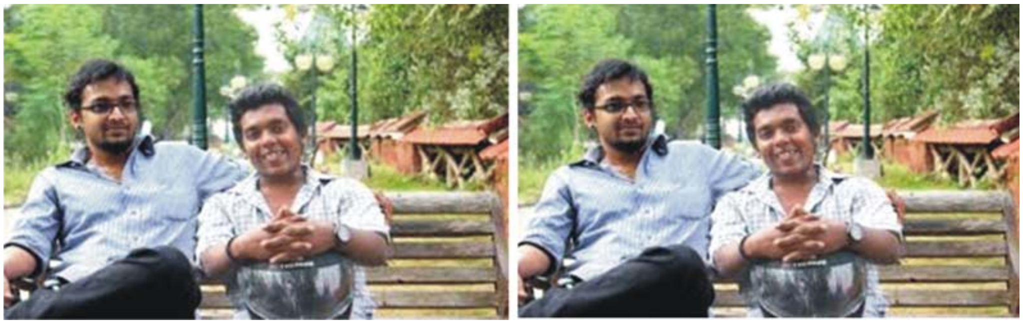
   To compute a dense set of localized illuminantcolor estimates, the input image is segmented into superpixels (*i.e.*, regions of approximately constantchromaticity) using the algorithm proposed in [6]. The color of the illuminantis estimated for super pixel mainly uses two separate illuminant colorestimators: the statistical generalized gray world estimatesand the physics-based inverse-intensity chromaticity space. In this work statistics-based IM estimation algorithms are used to obtain the illuminant map. According to [4] and [14], the original gray world hypotheses through the incorporation of three parameters are,

   a) **Derivative order *n* :** The assumption that the average of the illuminants is achromatic can be extended to theabsolute value of the sum of the derivatives of the image.

   b) **Minkowski norm *p* :** Instead of simply adding intensitiesor derivatives, respectively, greater robustness can beachieved by computing the*p*-thMinkowski norm ofthese values.

c) **Gaussian smoothing σ :** To reduce image noise, one cansmooth the image prior to processing with a Gaussiankernel of standard deviation. Putting these three aspects together, we estimate the colorof the illuminant '*e*' asilluminant map shown in Fig.2.

$$ke^{n,\,p,\,\sigma} = \left(\int \left| \frac{\partial \;\; f \;\; (x)}{\partial} \right| \; dx \right)^{1/}$$



(*a*) (*b*)

Figure 2: (*a*) Input image and (*b*) Illuminant map image

2. **Face Detection :** In this step, an automated face detector is employed to get the sole region of face [16]. This operator sets a bounding box around the region of face within the image. After finding all the faces from IMs, the proposed work crops each bounding box of face region for further processing. The sample result of face detection is shown in Fig. 3.

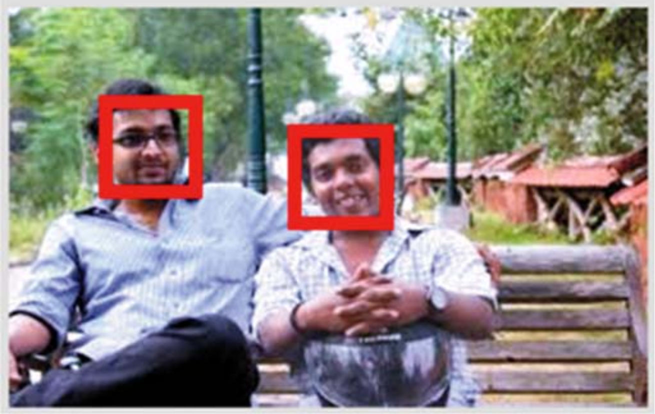


Figure 3: Faces detected in the illuminant map image

3. **Computation of Illuminant Features:** From each extracted face in the previous step, the proposed method needs to find telltales that allow identification of spliced images. Such information is present in different visual properties (*e.g.*, texture, shape, color) and becomes detectable when the suspicious images are transformed into an IM representation. Texture, for instance, allows us to characterize faces whereby illuminants are disposed similarly when comparing two faces. In this sense, GLCM statistical texture features are extracted from face regions.

   Differently from texture properties, shape properties present in IMs of fake faces, sometimes, have distinct pixel intensities when compared to shapes present in IMs of faces that originally belong to the analyzed image.According to Riess and Angelopoulou [4], when IMs are analyzed by an expert for detecting forgeries, the main observed feature is color. Thus, in this work it was decided to add color description techniques, extracted from the IMs transformed spaces, as an important visual cue to be encoded into the description process.

ACC is a technique based on color correlograms and encodes image spatial information. This color description technique is very robust when dealing with changes in appearance and shape, information that is indirectly represented in an IM, allowing us to compare faces in different positions. The BIC technique captures border and interior properties in an image and encodes them in a quantized histogram. It presented good performance in the study carried out by Penatti et al. [17]. Some color space models are more appropriate for extracting meaningful features than others depending on the target application. Therefore, given that some description techniques are more suitable for specific color spaces; this step converts illuminant maps into HSV color space representation.

4. **Classification:** The proposed work classifies the image as a forged one if any one faces in the image is found to be light inconsistent. Therefore, this step employs a Support Vector Machinealgorithm toclassify the feature vectors. SVM is a well knownsupervised category of machine learning algorithm; which exploits the kernel function to map the given data in higher dimension with feasibility to make the linearly inseparable data into linearly separable data [18]. In such a way, a hyper-plane is constructed with the maximum margin relating the two classes. The data vectors which are closer toward the hyper-plane are expressed as support vectors, which are alone, then classified into two classes.

5. **Localization of fake face:** The method for detecting the fake face, among all the faces in an image, selects the one with the highest probability to be the fake face. Given an image I classified as fake, the next step points out which part of the image is the result of a composition using Speeded Up Robust Features (SURF). It is becoming one of the most popular local feature detectorand descriptor in computer vision field [19]. The SURF detector is based on the Hessian matrix for itsgood performance in computational cost and accuracy.For a point (x, y) in an image I, The Hessian matrix H(σ)with is defined as

$$\mathrm{H}(\mathrm{x}, \sigma) = \begin{bmatrix} \mathrm{L}_{xx}(x,\sigma) & \mathrm{L}_{xy}(x,\sigma) \\ \mathrm{L}_{xy}(x,\sigma) & \mathrm{L}_{yy}(x,\sigma) \end{bmatrix}$$

The variable σ represents the Gaussian scale space at which thekeypoint exists. In SURF, a descriptor vector of length 64is constructed using a histogram of gradient orientationsin the local neighborhood around each keypoint.SURF first detects the interest points andgenerates corresponding descriptors form the fake face and from the whole input image. Then the matching points are identified and outliers are eliminated to preserve the inliers. Then region of fake image is highlighted on the whole input image.

4. RESULTS AND DISCUSSION

Evaluation Data: Tovalidate the proposed work,the datasetDSO-1 and DSI-1 areconsidered. DSO-1is composed of 200 indoor and outdoor imageswith 100 forged and 100 original images whose resolution is 2048 × 1535 pixels. DSI-1 composed by 25 original and 25 forged images of differentresolutions.

Performance Measures: To assess the performance of the proposed work, the metrics accuracy, sensitivity and specificity viz. are computed as follows:

$$\text{Accuracy} = \frac{tp + tn}{tp + fp + tn + fn}$$

$$\text{Sensitivity} = \frac{tp}{tp + fn}$$

$$\text{Specificity} = \frac{tn}{tn + fp}$$

Table 1
Confusion matrix representing splicing and authentic patterns

	Predicted	
Actual	Positive	Negative
Positive	True positive *tp*	False positive *fp*
Negative	False negative *fn*	True negative *tn*

where, *tp*, *fp*, *tn* and *fn* are defined in the confusion matrix given in Table 1.

The performance measure sensitivity represents the probability of the fake images (probability of true positives) that are declared by the testing procedure, specificity denotes the probability of authentic images (probability of true negatives) that are declared by the testing procedure, whereas accuracy represents the overall quality of the classification system which is a balanced measure between the positive and negative cases.

5. EXPERIMENTAL RESULTS

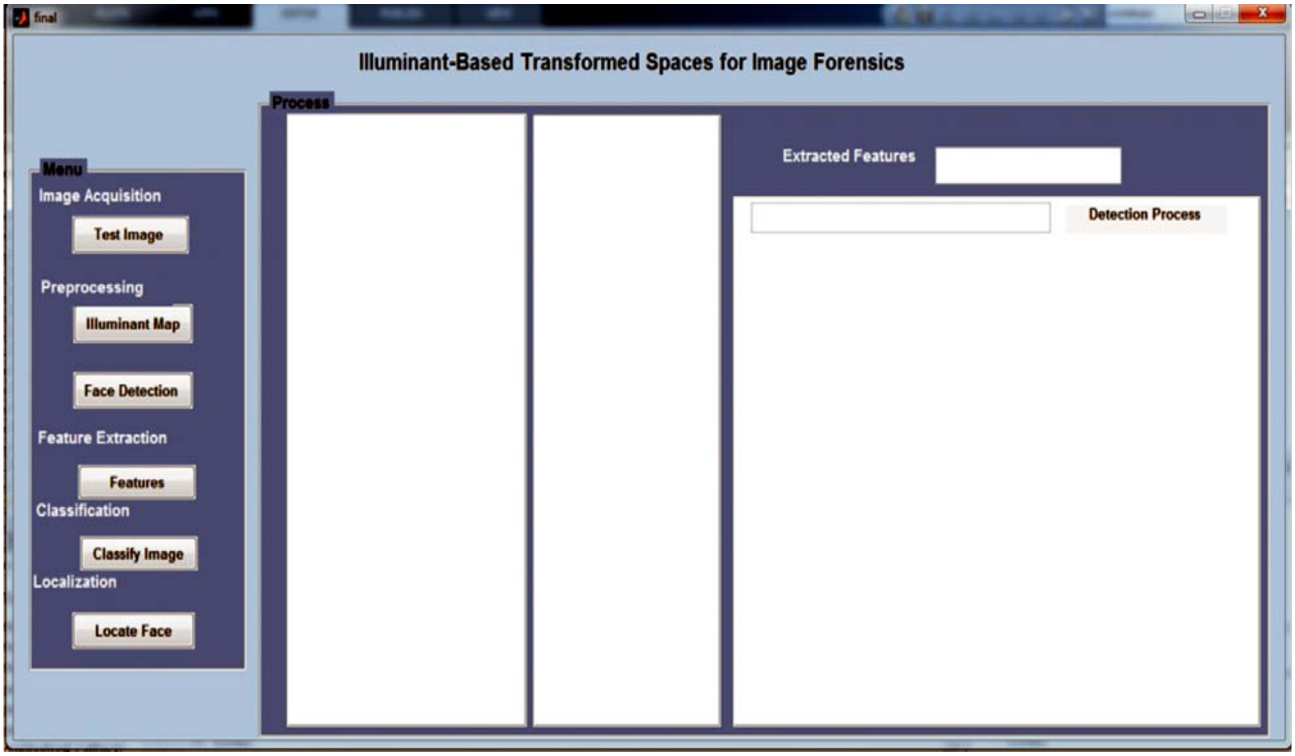
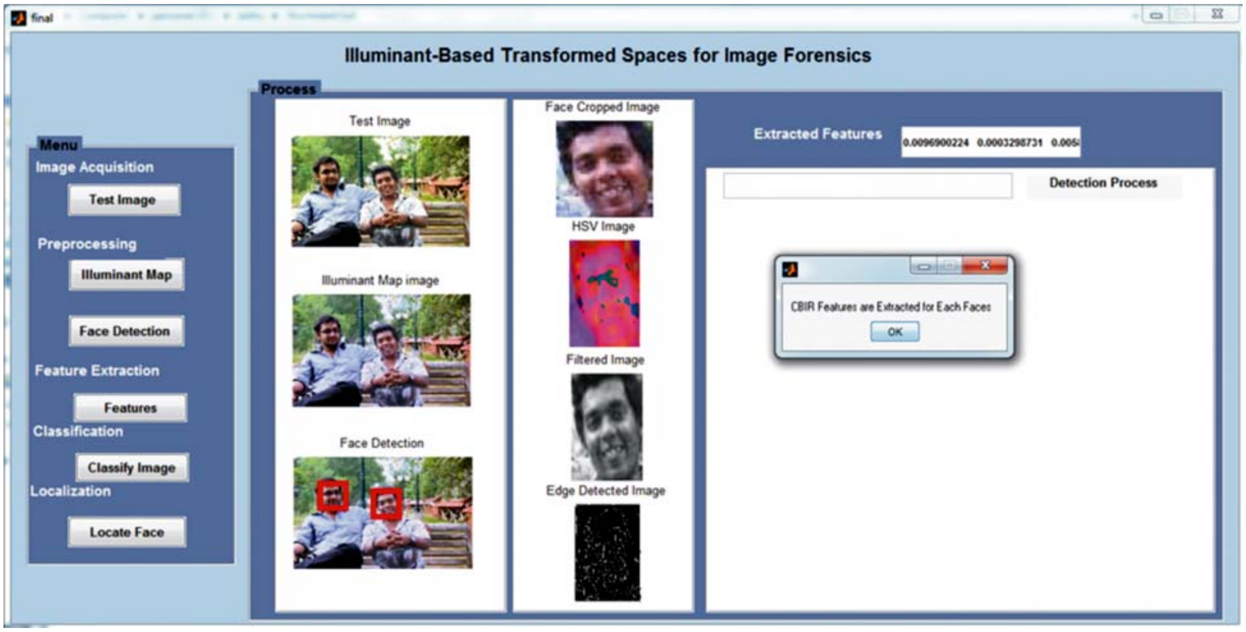


Figure 4: Graphical User Interface Initial Screen

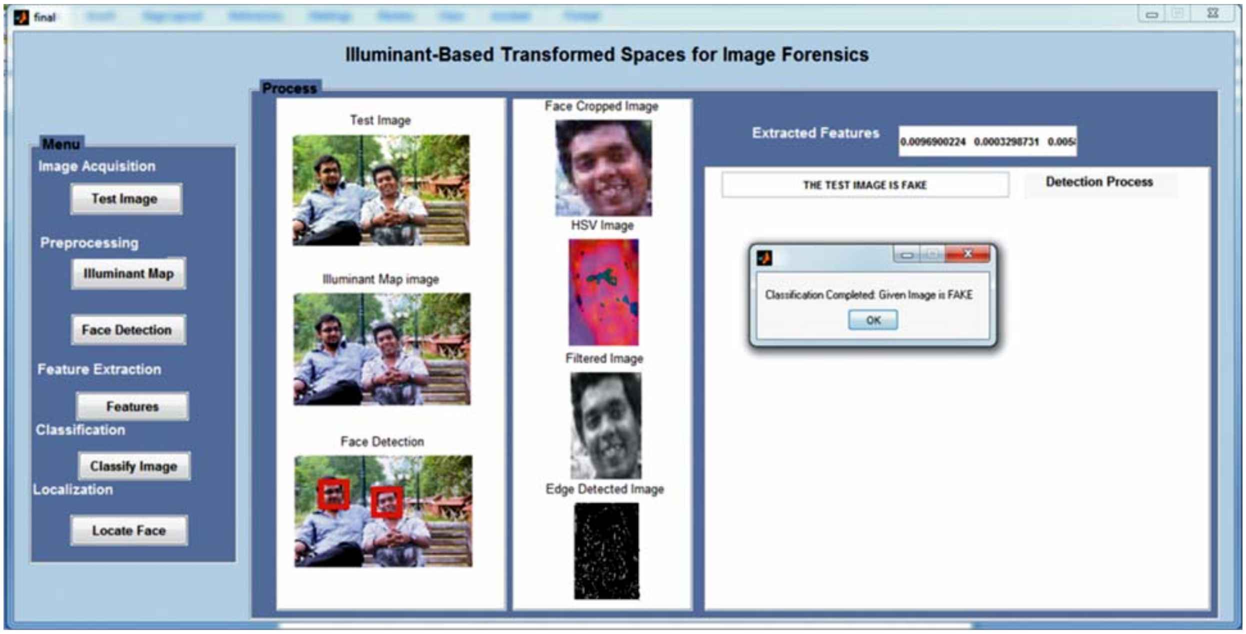
To find the forged images, color features such as color HSV histogram, auto-correlation and color moment features are extracted. Energy, contrast, correlation and homogeneity texture features and edge based shape features are also extracted. The features extracted from each detected faces are encoded as pair of feature vectors and fed as input to the SVM to classify fake images.The radial basis function kernel of SVM is obtained the finer results.The sample results are shown in Fig.4 – Fig.7. Fig. 4 shows the user interface created for the proposed forgery detection; Fig. 5 shows the snapshot of features extraction from detected faces. The screen shown in Fig.6proves that the proposed work correctly classifies as fake image for the given input of forged one and Fig. 7 exhibits the localized region of fake face.



Extracted Features: 0.0096900224 0.0003298731 0.005

CBIR Features are Extracted for Each Faces

Figure 5: Features extracted from the input image by the proposed method

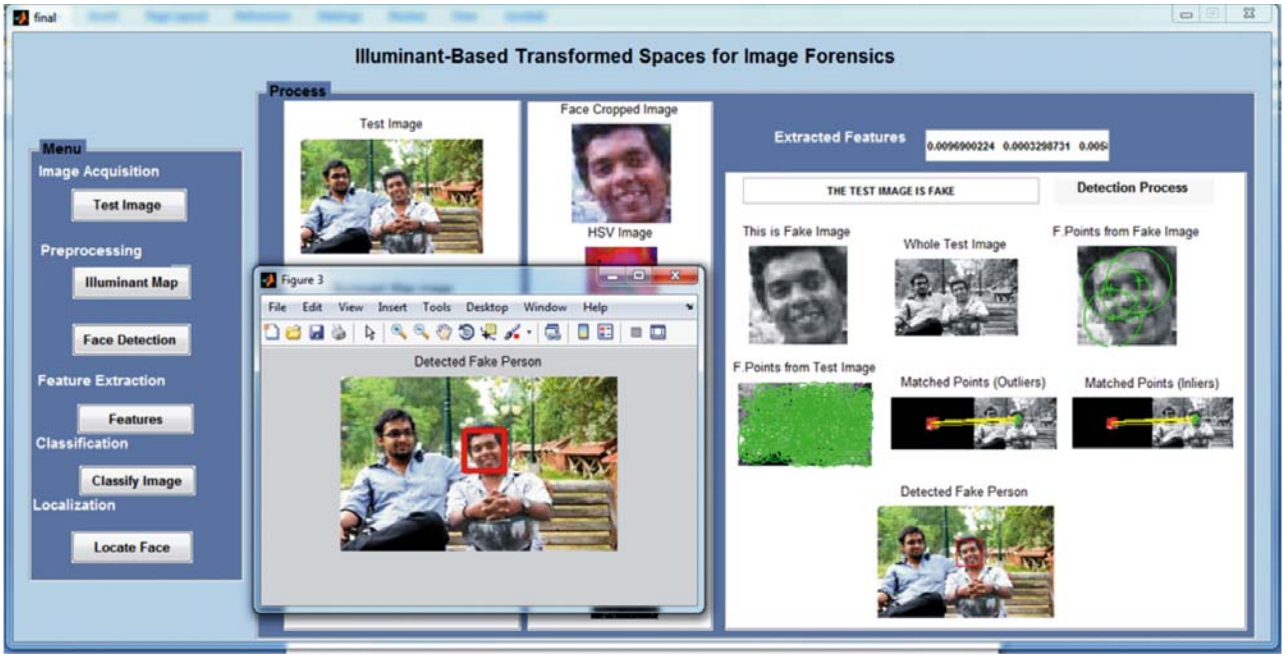


Extracted Features: 0.0096900224 0.0003298731 0.005

THE TEST IMAGE IS FAKE

Classification Completed: Given Image is FAKE

Figure 6: Image detected as fake by the proposed method



0.0096900224 0.0003298731 0.005

THE TEST IMAGE IS FAKE

Figure 7: Localizedregion of fake face by the proposed method

Table 2
Performance of proposed work on DSO-1 and DSI-1 datasets

Dataset	*Accuracy*	*Sensitivity*	*Specificity*
DSO-1	82.50	81.55	83.50
DSI-1	84.00	81.48	86.95

To validate the performance, the experiment is carried out on the datasets DSO-1 and DSI-1. The performances are evaluated in terms of accuracy, specificity and sensitivity and are tabulated in Table 2. The proposed work produced a better result of 82.50%, 81.55% and 83.50% in terms of accuracy, sensitivity and specificity on DSO-1 dataset. It is also obtained 84% of accuracy, 81.48% of sensitivity and 86.95% of specificity on DSI-1 dataset.

6. CONCLUSION

This work aims at detecting image forgeries containing people and present a method for locating the forgery, specifically, the face of a person in an image. Illuminant properties of image descriptors such as color, texture and shape features were extracted and supervised algorithm of SVM is utilized to classify the images. SURF features were also extracted to focus the region of fake face in the image. The tests were carried out on two data sets (DSO-1 and DSI-1) and also performances were appraised by accuracy, sensitivity and specificity. The test results were exhibited that the proposed work has obtained a better results.

REFERENCES

[1] 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, Jul. 2013.

[2] Vaishnavi, Dharmalingam, and T. S. Subashini. “A passive technique for image forgery detection using contrast context histogram features.” International Journal of Electronic Security and Digital Forensics 7.3 (2015): 278-289.

[3] A. Pinto, W. Robson Schwartz, H. Pedrini, and A. De Rezende Rocha, “Using visual rhythms for detecting video-based facial spoof attacks,” IEEE Trans. Inf. Forensics Security, vol. 10, no. 5, pp. 1025–1038, May 2015.

[4] C. Riess and E. Angelopoulou, “Scene illumination as an indicator of image manipulation,” in Proc. Inf. Hiding Workshop, vol. 6387. 2010, pp. 66–80.

[5] E. Kee, J. F. O’brien, and H. Farid, “Exposing photo manipulation with inconsistent shadows,” ACM Trans. Graph., vol. 32, no. 3, pp. 28:1–28:12, Jul. 2013.

[6] E. Kee and H. Farid, “Exposing digital forgeries from 3-D lighting environments,” in Proc. IEEE Int. Workshop Inf. Forensics Secur., Dec. 2010, pp. 1–6.

[7] M. K. Johnson and H. Farid, “Exposing digital forgeries by detecting inconsistencies in lighting,” in Proc. ACM 7th Workshop Multimedia Secur., New York, NY, USA, 2005, pp. 1–10.

[8] W. Fan, K. Wang, F. Cayre, and Z. Xiong, “3D lighting-based image forgery detection using shape-from-shading,” in Proc. 20th Eur. Signal Process. Conf., Aug. 2012, pp. 1777–1781.

[9] Vaishnavi, D., and T. S. Subashini. “Recognizing image splicing forgeries using histogram features.” Big Data and Smart City (ICBDSC), 2016 3rd MEC International Conference on. IEEE, 2016.

[10] S. Gholap and P. K. Bora, “Illuminant colour based image forensics,” in Proc. IEEE Region 10 Conf., Nov. 2008, pp. 1–5.

[11] 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.

[12] K. Francis, S. Gholap, and P. K. Bora, “Illuminant colour based image forensics using mismatch in human skin highlights,” in Proc. Nat. Conf. Commun., Feb./Mar. 2014, pp. 1–6.

[13] X. Wu and Z. Fang, “Image splicing detection using illuminant color inconsistency,” in Proc. 3rd Int. Conf. Multimedia Inf. Netw. Secur., Nov. 2011, pp. 600–603.

[14] 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.

[15] A. Gijsenij and T. Gevers, “Color constancy using natural image statistics and scene semantics,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 33, no. 4, pp. 687–698, Apr. 2011.

[16] Viola, Paul, and Michael J. Jones. “Robust real-time face detection.” International journal of computer vision 57.2 (2004): 137-154.

[17] O. A. B. Penatti, E. Valle, and R. da Silva Torres, “Comparative study of global color and texture descriptors for Web image retrieval,” J. Vis. Commun. Image Represent., vol. 23, no. 2, pp. 359–380, 2012.

[18] V. N. Vapnik and V. Vapnik, Statistical learning theory, vol. 1. Wiley New York, 1998.

[19] Bay, Herbert, TinneTuytelaars, and Luc Van Gool. “Surf: Speeded up robust features.” European conference on computer vision. Springer Berlin Heidelberg, 2006.