Fake Color Image Detection Using Histogram And Gaussian Mixture Model

Aashmi Miranda .S[1], Dr.K.Thulasimani[2]
[1]Dept of Computer Science and Engineering
[2]Associate Professor, Dept of Computer Science and Engineering
[1, 2] Government College of Engineering, Tirunelveli

Abstract- *Image forgery implies altering the digital image to some meaningful or valuable data. Image forensics is a well developed field that analyzes the images of specific conditions to build up trust and genuineness. Although image editing techniques can provide significant aesthetic or entertainment value, they may also be used with malicious intent .An emerging image editing technique is colorization, in which gray scale images are colorized with realistic colors. But this technique may also be intentionally applied to certain images to confound object recognition algorithms. In this work, it is observed that, colorized images. However, image editing techniques develop over time. Image retouching techniques usually change the images using a variety of mechanisms. The digital image developed from the colorization Method possess statistical differences in their hue and saturation channels and also need to observe statistical inconsistencies in the dark and bright channels, because the colorization process will effectively affect the dark and bright channel values. Based on the observations, that is potential traces in the hue, saturation, dark and bright channels, two simple yet effective detection method are proposed for detecting the fake colorized images: Histogram based Fake Colorized Image Detection (FCID-HIST) by using the histogram features of the hue saturation dark channel and bright channel and Feature Encoding based Fake Colorized Image Detection (FCID-FE).*

Keywords- image forgery, image detection, histogram, feature encoding

I. INTRODUCTION

Digital Image forensics is a emerging field which aims to check the originality of digital images by recovering information about their past. Digital images are easily get affected by various methods, which lead to change their meaning and its original state of image. With the huge development of technology, the usage of the image has been expanding day by day in our daily lives. Because of this, forgery of the digital image has turned out to be increasingly straightforward and indiscoverable

Image forensics is a well developed field that analyzes the images of specific conditions to build up trust and genuineness. and protection assert investigations.

It is quick and better-known domain due to several executions of real-time applications in numerous areas incorporates intelligence, sports, legitimate administrations, news reporting, medical imaging,

Image Forgery techniques classified into two classes, active and passive techniques. The active techniques initially refer to techniques which join with watermark to which hide authentication information in the to-be protected images .When the integrities of these images demand verification, watermark extraction procedures The original images are compared to the watermark images to detect forgeries. Since the active techniques require the watermark to be embedded and the prior to detection are limited in their applications. The imperceptible forged image detection is exceptionally complex. Any forgery detection method creates a correlation among the forged image and the original image to lead successful forgery detection. The observation shows the various image forgery detection techniques. A few main forgery detection methods are presented for second image forgery detection. The significant image forgery detection algorithms fall in any one of the categories.

Our proposed methods belong Passive image forgery detection approaches, to which, usually detect the manipulations to the input images directly. Passive image forgery (editing) detection techniques have mainly focused on the three detection techniques. If these images are checked by humans, the cost increases importantly as the number of to-be-examined images increases in the basic need. Intentionally, detection via human eyes is difficult for the big data is the bigger problem.. On the other side o, conventional image forgery detection techniques are developed with different assumptions that may not be appropriate for generated fake image detection. Therefore a detailed study of the fake colorized images is to be done..

II. BACKGROUND

Forgery detection has been investigated for a period of ten years. Generally, forgery detection exhibits different characteristics of images and attempts to find traces to analyze the results. As the observation shows, most of the traditional forgery detection techniques mainly classified into three types, copy-move , photomontage and image retouching detection.

Copy-move detection relies on identifying duplicated regions in a tampered image. Initally, these techniques used to seek an appropriate feature in a particular domain, such that the detection can be performed with searching the most similar two units (such as patches). Different methods usually exploit different features. [1] explores features in the frequency domain by dividing the image into overlapping blocks and detects the copy-move forgery via matching the quantized discrete cosine transform (DCT) coefficients. [2] performs a rotation invariant detection based on the Fourier-Mellin transform. [3]localizes the duplicated regions based on the Zernike moments, which exhibit the rotation invariance property, of small image blocks. [3] reports decent results especially when the duplicated regions are smooth. [4] uses the famous SIFT feature [5] to find multiple duplicated regions and the geometric transformation performed by the copy-move operation is estimated. [6] shows a SIFT based detection method by arranging and comparing the SIFT features with a broad first search neighbors clustering algorithm and distinguishing the duplicated origins from the tampered regions via CFA features. [7] develops a hierarchical SIFT-based key point matching technique to solve a problem of previous key point matching based detection techniques, which allows to give poor performances when the copy-moved regions are small or smooth.

As we are living in the today’s computerized world in which all kind of advancement is getting to be conceivable and in the meantime the utilization of pictures have been expanding day by day in our lives

By summarizing each techniques it has been known that there are more techniques to detect the traditional forgery techniques , and it has been decided to propose the technique to detect the image forgery based on the colorization.

III. METHODOLOGY

The rapid development in colorization techniques has formed colorized images to be visually not distinguishable from natural images. Traditional colorization methods are already experts of misleading human observers in the subjective tests. To identify the fake colorized images from the natural images, the detailed study of the statistics of the fake colorized images, which are generated by traditional methods has tto be performed and two effective detection schemes has been proposed, FCID-HIST and FCID-FE. According to the observation, the colorized images has less saturated colors, and the colorization method overlaps one color over the other, based on these differences it is difficult to identify by the human eyes.

The Hue-Saturation Value (HSV) color space represents the chrominance information in the hue and saturation channel separately, hence we calculate the normalized histograms (each containing 250 bins) of the hue and saturation channel in natural images and their corresponding fake colorized images, separately, as shown in Fig. 1

In this dark channel priors and the bright channel priors are taken as the channel priors feature. In the dark channel prior, the dark channel of a natural image is minimum i.e(is close to zero), and in the bright channel prior, the bright channel of a natural image is maximum i.e.(is close to 255). The dark channel I_{dc} and bright channel I_{bc} of an image I are defined as shown below.

$$I_{dc} = \min_{y \epsilon \Omega(x)} \left(\min_{cp \epsilon (r,g,b)} \left(I_{cp}(y) \right) \right) \qquad (1)$$

$$I_{bc} = \max_{y \epsilon \Omega(x)} \left(\max_{cp \epsilon (r,g,b)} \left(I_{cp}(y) \right) \right) \qquad (2)$$

where x denotes the pixel location, Icp stands for a color channel of I and Ω(x) shows the local patch centered at the location x.

A. FCID-HIST

By observing the statistical differences the effective technique to detect the fake colorized images i.e. histogram based fake colorized image detection has been proposed.

In FCID-HIST four features are used to detect the forgeries they are the hue feature F_h, the saturation feature F_s, the dark channel feature F_{dc} and the bright channel feature F_{bc}.

The hue feature is extracted from the hue channel histogram distributions. Let K_h be the total number of bins in hue channel histogram distribution $Dist_{h,n}$ and $Dist_{h,f}$, be the normalized hue channel histogram distribution for the natural and fake training images, respectively, and $Dist_h^\alpha$ denotes the corresponding histogram for the αth input image, which can be a training or testing image.. Let the most distinctive bin be the

$\mathrm{Dist}_h^{\alpha}(v_h)$.The index of the most distinctive bin for the hue channel (v_h). can be calculated as follows:

$$v_h = \mathrm{argmax}_x \, \| \mathrm{Dist}_{h,n}(x) - \mathrm{Dist}_{h,f}(x) \|_2$$

$$v_h = \underset{x}{\mathrm{argmax}} \, | \underset{h,n}{\mathrm{Dist}}(x) - \underset{h,f}{\mathrm{Dist}}(x) | \qquad (3)$$

After calculating the index value the first order derivative i.e the first order hue features can be extracted.

$$F_h^{\alpha}(1) = \mathrm{Dist}_h^{\alpha}(v_h) \qquad (4)$$

The Distributions may vary according to their bins the second order derivative of the hue feature can be found by the

$\mathrm{DistD}_{\alpha}{}^{h}(l) = \mathrm{Dist}_{\alpha}{}^{h}(l + 1) - \mathrm{Dist}_{\alpha}{}^{h}(l)$ to know the variation in the distribution of the histogram

$$F_h^{\alpha} = \sum_{l=1}^{k_h-1} |DistD_h^{\alpha}(l)| \qquad (5)$$

The hue feature formed by combination of the first order and the second order derivative of the hue channel.

$$F_{\alpha}{}^{h} = [F_{\alpha}{}^{h}(1) \; F_{\alpha}{}^{h}(2)] \qquad (6)$$

The process will be repeated to find the saturation feature $F^{\alpha}{}_{s}$,the dark channel feature $F^{\alpha}{}_{dc}$ and the bright channel feature $F^{\alpha}{}_{bc}$ by using the histogram distributions ($\mathrm{Dist}_{s,n}$, $\mathrm{Dist}_{s,f}$), ($\mathrm{Dist}_{dc,n}$, $\mathrm{Dist}_{dc,f}$), and ($\mathrm{Dist}_{bc,n}$, $\mathrm{Dist}_{bc,f}$) channels of the training images.

When all the features are calculated the final detected histogram feature $F_{HIST}{}^{\alpha}$ for the training images can be formed as

$$F^{\alpha}{}_{HIST} = [F^{\alpha}{}_{h} \; F^{\alpha}{}_{s} \; F^{\alpha}{}_{dc} \; F^{\alpha}{}_{bc}] \qquad (7)$$

After calculating the detected feature, FCID-HIST uses the supporting vector machine (SVM) for training and classifying the fake colorized images and the real images based on the prediction formed.

B. FCID-FE

Even though the FCID-HIST produces the decent performance but the features extracted will not completely utilize the statistical difference formed from the histograms. So a new technique has been proposed i.e Feature Encoding based Fake Colorized Image Detection (FCID-FE).

The hue, saturation, dark and bright channels of a training image can be represented as $I^{\beta}{}_{h}$, $I^{\beta}{}_{s}$, $I^{\beta}{}_{dc}$ and $I^{\beta}{}_{bc}$ respectively, where β is the index of the image. The training sample set ϕ is created by using the following equation

$$\Phi((z - 1) * I * j + (i - 1) * j + j)$$
$$=[I^{\beta}{}_{h}(i, j) \; I^{\beta}{}_{s}(i, j) \; I^{\beta}{}_{dc}(i, j) \; I^{\beta}{}_{bc}(i, j)] \qquad (8)$$

In comparing to the histogram modeling FCID-FE models the Gaussian mixture model with the sample data distribution G created using the above equation

$$G\left(\frac{\phi}{\theta}\right) = \sum_{n=1}^{N} \log p\left(\frac{\phi_n}{\theta}\right) \qquad (9)$$

where N shows the number of samples in Φ, Θ represents for the parameter set of the GMM and Θ is defined as follows

$$\Theta = \omega_a, \mu_a, \sigma_a, a = 1, \ldots, N_m, \sum_{n=1}^{N_m} \omega_a = 1 \quad (10)$$

where ω_a stands for the weight, μ_a represents the mean value vector, σ_a shows the covariance matrix and N_m is the number of Gaussian distributions in the distribution model. Then, the likelihood function of Φ_n being formed by the GMM Θ can be modeled as given below

$$\rho\left(\frac{\phi_n}{\theta}\right) = \sum_{m=1}^{N_m} \log \omega_m \rho_m\left(\frac{\phi_m}{\theta}\right) \qquad (11)$$

Where $\rho_m\left(\frac{\phi_m}{\theta}\right)$ is defined as given below

$$\rho_m\left(\frac{\phi_m}{\theta}\right) = \frac{exp\left[-\left(\frac{1}{2}\right)(\phi_m - \mu_a)^T \sigma_a^{-1} (\phi_m - \mu_a)\right]}{2\pi^{\frac{N_v}{2}} |\sigma_a|^{\frac{1}{2}}} \qquad (12)$$

where N_v shows the number of dimensions of each generated sample vector. Then, GMM can be developed by using the parameter set Θ. With the constructed GMM, FCID-FE uses different moments of the distribution and encodes each subset Φ^{β} of the sample vectors, of each training image, into training fisher vector values and the fisher vector can be expressed as follows

$$F_{FE}^{\beta} = \left[\frac{\lambda_1 \delta G\left(\frac{\varphi^{\beta}}{\theta}\right)}{\delta \omega_a} \; \frac{\lambda_2 \delta G\left(\frac{\varphi^{\beta}}{\theta}\right)}{\delta \mu_{a,v}} \; \frac{\lambda_3 \delta G\left(\frac{\varphi^{\beta}}{\theta}\right)}{\delta \sigma_{a,v}} \right] \qquad (13)$$

where v = 1,2,...,N_v and λ_1, λ_2 and λ_3 are expressed in the following equations ,where λ_1, λ_2 and λ_3 are fisher vector values that are encoded from the inputs given.

$$\lambda_1 = \left(N\left(\frac{1}{\omega_a} + \frac{1}{\omega_1}\right)\right)^{\frac{-1}{2}} \qquad (14)$$

$$\lambda_2 = \left(\frac{N\omega_a}{(\sigma_{a,v})^2}\right)^{\frac{-1}{2}} \qquad (15)$$

$$\lambda_3 = \left(\frac{2N\omega_a}{(\sigma_{a,v})^2}\right)^{\frac{-1}{2}} \qquad (16)$$

SVM is used as the training classifier. For testing, in FCID-FE the training test sample will be constructed then the Gaussian mixture model is used to encode the image into the fisher vector. Finally the features are trained with the svm classifier to detect the fake images. When comparing to the two algorithms proposed the second algorithm gives the slightly better results with the half total error rate of the 4.67.

C. SVM Classifier

Support vector machines (SVMs) is supervised learning methods used for classification, regression and outliers detection. svm classifier is used to classify the image by using the binary classification 0 and 1. Svm classify the images based on the prediction outcome produced by using the features extracted from the images. If the prediction gives 0 the it is a fake image and if it produces the outcome prediction of 1 then it is the original image.

IV. EXPERIMENTAL RESULTS

This area shows about the databases and the measurements , experiment results are shown detailed accordingly.

A. Setups and Measurements

In this work, SVM, is implemented for classification and to get the predicted results. The VLFeat software is to be used for the GMM modeling and Fisher vector encoding. In the work two performance measure is to used to evaluate the performances, one is the half total error rate (HTER) measurement and the other is the receiver operating characteristic (ROC)

HTER is defined in as follows.

$$\text{HTER} = \frac{FPR+FNR}{2}$$

$$= \frac{\frac{FP}{(TN+FP)}+\frac{FN}{(TP+FN)}}{2} \qquad (17)$$

Where P represents the positive samples, N represents the negative samples. The natural images and the fake images are denoted as the positive and the negative samples.

B. Databases

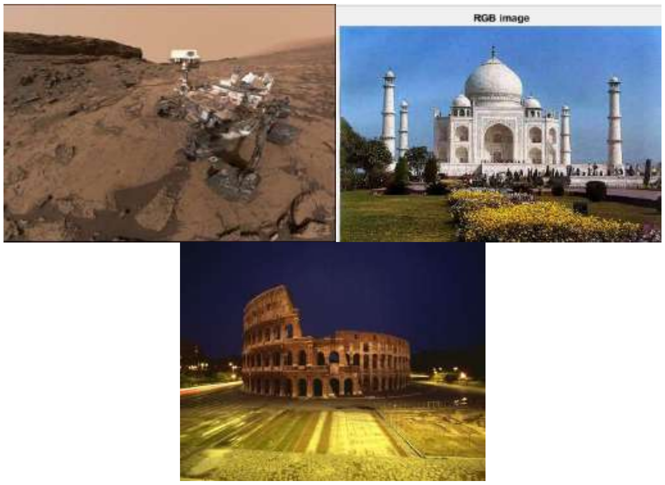
For the best results of the proposed methods, different databases are used. For the evaluation of the proposed algorithms it has been used a open image dataset which contains more than 2000 images. In the total number of images 80 % of the images are given as the training images and the remaining images are used for the testing The image has an resolution of 600 * 600.The images are the natural images and their respective fake images. The natural images in database include various types of images, such as animals, human, furniture and outdoor scenes.

C. Results

The dataset which contains the real and their fake images are obtained and they will undergo both the training and the testing .The images are loaded and they have been to transformed to hsv image to find the hue saturation and the value images and their respective histograms. Then the dark channel and the bright channel of the images and their respective histograms are found.

Then the features is extracted and are given to the GMM to produce the samples then they process with the GMM and produce the fisher vector values and it undergoes for the svm classifier and classify whether the image is real or fake. Finally analysis of the project will be done. Analysis process makes the project more efficient. The performance and accuracy of the algorithm are analyzed using the above measures.

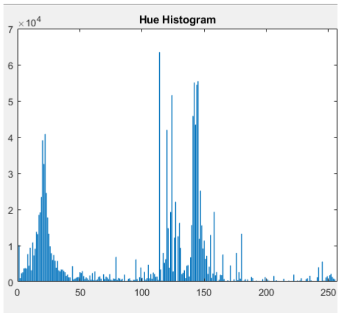
(a)



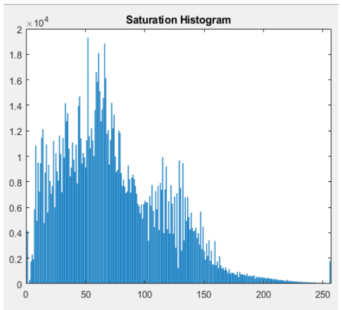
(b)

Fig. 1: (a) Real images. (b) Fake colorized image

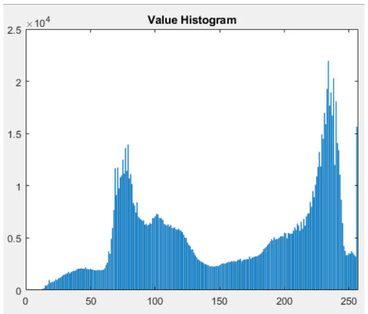
Histogram distributions (hue ,saturation , value, natural images)



(a)

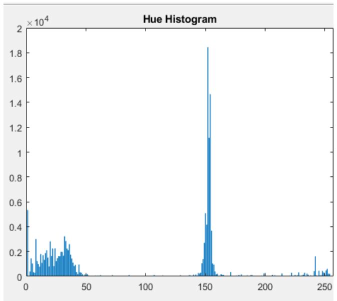


(b)

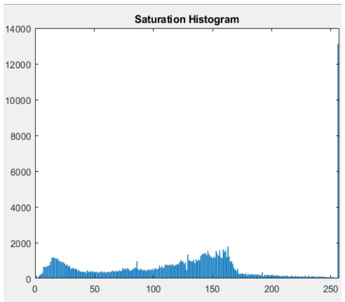


(c)

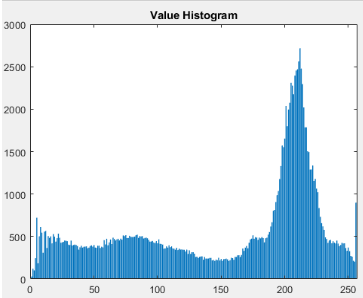
Histogram distributions (hue ,saturation , value, fake images)



(d)



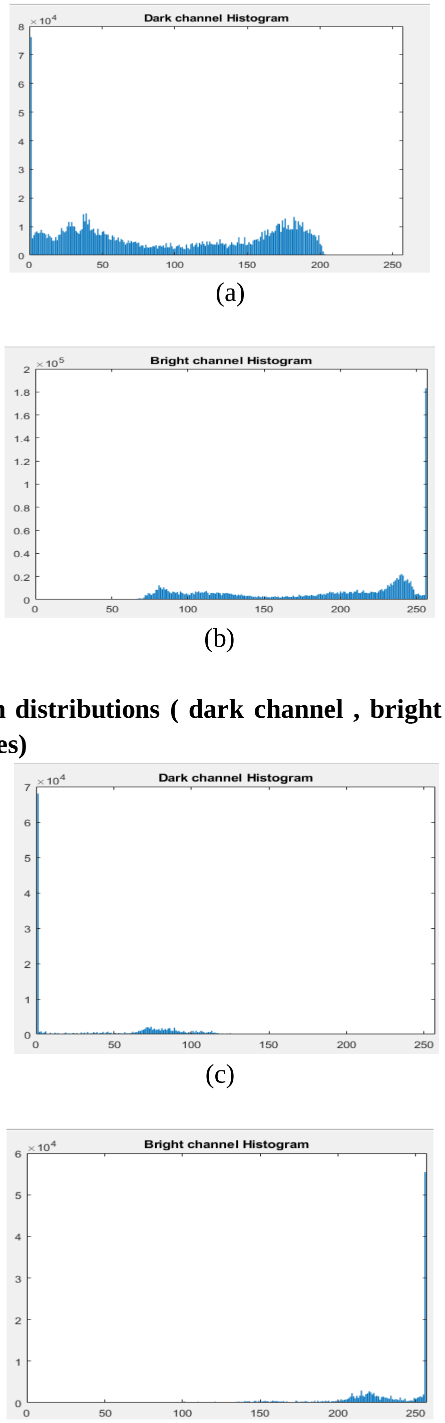
(e)



(f)

Fig. 3: (a)Hue Histogram Distribution (natural images). (b) Saturation Histogram Distribution (natural images). (c) Value Histogram Distribution (natural images). (d) Hue Histogram Distribution (fake images). (e) Saturation Histogram Distribution (fake images). (f) Value Histogram Distribution (fake images)

Histogram distributions (dark channel , bright channel , natural images)



(a)

(b)

Histogram distributions (dark channel , bright channel , fake images)

(c)

(d)

Fig. 4: (a) Dark channel Histogram distribution (natural images). (b) Bright channel Histogram distribution (natural images).(c) Dark channel Histogram distribution (fake images). (d) Bright channel Histogram distribution (fake images)

V. CONCLUSION AND DISCUSSION

In this project, histogram based fake colorized image detection and the feature encoding based fake colorized image detection has been proposed to identify the fake colorized images. . The work produces an accuracy of 87%.So these algorithms are used in the field of image forgery detection to get better performance for finding the fake images.

Although the proposed FCID-HIST and FCID-FE gives decent performances in the experiments, this work is only a initial performance or the initial trail, and there are many ways or techniques for future studies that require further exploration.

The performance of current methods sometimes decreases obviously when the training images and the testing images are generated from different traditional methods or different datasets, thus blind fake colorized image detection features and methods may be developed in the future by studying the common characteristics of other colorization techniques and the channels features and also the algorithm will be well tuned for the further process. Moreover, better feature encoding approaches can be considered for improving performance, as well as the optimization of the detection features and parameters to improve the custom features constructed.

REFERENCES

[1] H. Farid, “Exposing digital forgeries from JPEG ghosts,” *IEEE Trans.Inf. Forensics and Security*, vol. 4, no. 1, pp. 154-160, 2009.

[2] J. Li, X. Li, B. Yang and X. Sun, “Segmentation-Based Image Copy-Move Forgery Detection Scheme,” *IEEE Trans. Inf. Forensics and Security*, vol. 10, no. 3, pp. 507-518, 2015.

[3] G. Cao, Y. Zhao, R. Ni and X. Li, “Contrast Enhancement-Based Forensics in Digital Images,” *IEEE Trans. Inf. Forensics and Security*, vol. 9, no. 3, pp. 515-525, 2014.

[4] G. Larsson, M. Maire and G. Shakhnarovich, “Learning representations for automatic colorization,” *in Proc. European Conf. Comp. Vision (ECCV)*, pp. 577-593, 2016.

[5] I.J. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville and Y. Bengio, “Generative adversarial nets,” *in Procs. Advances in Neural Inf. Process. Systems (NIPS)*, pp. 2672-2680, 2014.

[6] F. Huang, X. Qu, H.J. Kim and J. Huang, “Reversible data hiding in JPEG images,” *IEEE Trans. Circuits and Systems for Video Technology*, vol. 26, no. 9, pp. 1610-1621, 2016.

[7] J. Yin, R. Wang, Y. Guo and F. Liu, “An adaptive reversible data hiding scheme for JPEG images,” *in Proc.*

Int. Workshop on Digital-Forensics and Watermarking (IWDW), pp. 456-469, 2016

[8] J. Wang, S. Lian and Y.-Q. Shi, ”Hybrid multiplicative multi watermarking in DWT domain”, *Multidimensional Systems and Signal Process.*, vol. 28, no. 2, pp. 617C636, 2017.

[9] Y. Yang, W. Ren, Y. Guo, R. Wang and X. Cao, “Image deblurring via extreme channels prior,” *in Procs. IEEE Int. Conf. Comp. Vision and Pattern Recognition (CVPR)*, 2017, Accepted.

[10] J. Farquhar, S. Szedmak, H. Meng and J. Shawe-Taylor, “Improving ”bag-of-keypoints” image categorization,” *Technical report, University of Southampton*, 2005.

[11] A. Levin, D. Lischinski and Y.Weiss, “Colorization using optimization,” ACM Trans. Graphics, vol. 23, no. 3, pp. 689-694, 2004.

[12] J. Pang, O.C. Au, K. Tang and Y. Guo, “Image colorization using sparse representation,” in Proc. IEEE Int. Conf. Acoustics, Speech and Signal Process. (ICASSP), pp. 1578-1582, 2013.

[13] G. Charpiat, M. Hofmann and B. Scholkopf, “Automatic image colorization via multimodal predictions,” in Proc. European Conf. Comp. Vision (ECCV), pp. 126-139, 2008.

[14] X. Chen, J. Li, D. Zou and Q. Zhao, “Learn Sparse Dictionaries for Edit Propagation,” IEEE Trans. Image Process., vol. 25, no. 4, pp. 1688-1698, 2016.

[15] Y. Li and J. Zhou, “Image copy-move forgery detection using hierarchical feature point matching,” in Proc. Asia-Pacific Signal and Inf. Process. Association Annual Summit and Conf. (APSIPA ASC), pp. 1-4, 2016.