EasyChair Preprint

№ 6025

Histogram and Feature Encoding Based Fake Colorized Image Detection Using Machine Learning

Yogesh Gaikwad and Jaishree Waghmare

July 6, 2021

Histogram and Feature Encoding and Extraction based Fake Colorized Image Detection

Mr. Yogesh J. Gaikwad
Student, Department of Computer Engineering
Trinity College of Engineering & Research, Pune.
E-mail: yogesh.gaikwad87@gmail.com

Mrs. Jaishree G. Waghmare
Asst. Professor Department of Computer Engineering, Trinity College of Engineering & Research, Pune.
E-mail: jaishreewaghmare@gmail.com

Abstract—

Image forensics aims to notice the manipulation of Digital pictures. Currently, splicing detection, copy-move detection and image retouching detection are attracting significant attentions from researchers. An emerging image editing technique is colorization, in which grayscale images are colorized with realistic colors. Unfortunately, this system may be by design applied to bound pictures to confound seeing algorithms. To the simplest of our information, no forensic technique has yet been invented to identify whether an image is colorized. We observed that, compared to natural pictures, colorized images, which are generated by three state-of-the-art methods, possess statistical differences for the hue and saturation channels. Besides, we also observe applied mathematics inconsistencies within the dark and bright channels, as a result of the colorization method can inevitably have an effect on the dark and bright channel values.

We propose two simple yet effective detection methods for fake colorized images: Histogram based Fake Colorized Image Detection (FCID-HIST) and Feature Encoding based Fake Colorized Image Detection (FCID-FE) with Machine Learning. Experimental results demonstrate that each projected ways exhibit a good performance against multiple progressive colorization approaches.

Keywords: - Image Forgery Detection, Fake Colorized Image Detection, Hue, Saturation

I. Introduction

The rapid amount of image editing technologies has increased both the ease with which images can be manipulated and the difficulty in distinguishing between altered and natural images. In addition to the conventional image editing techniques like splice [1], copy-move [2] and retouching [3], a lot of image redaction techniques, such as colorization [4] and image generation [5], are proposed. Since these types of image editing techniques generate new content with/without references, we tend to denote them because the generative image redaction techniques.

Although image editing techniques can provide significant aesthetic or diversion worth, they'll even be used with malicious intent. In general, various image editing approaches employ different mechanisms. Image retouching techniques sometimes modification the pictures via a spread of mechanisms. Among the generative image writing techniques, image generation usually produces a meaningful image from a noise vector with/without some additional information such as text or a class label. Colorization, on the other hand, usually colorizes images with visually plausible colors, which may cause misjudgment when specific objects/scenes must be identified/tracked.

Fortunately, various image rhetorical technologies are developed within the past decades. According to their Mechanisms and applications, they can be categorized into Two classes,

1. Active techniques
2. Passive techniques.

The Active techniques usually refer to watermarking techniques [6-8], which embed authentication information in the to-be protected images. When the integrities of these images demand verification, watermark extraction procedures are performed and the extracted watermarks are compared to the first watermark to detect forgeries. Since the active techniques require the watermark to be embedded before detection, the Applications, in practice, are limited.

In contrast, passive image fake detection approaches, to that our projected ways belong, typically notice the Manipulations to the input images directly. Traditionally, passive image forgery detection techniques have mainly focused on conjunction detection [1], copy-move detection [2] and image retouching detection [3]. To the best of our knowledge, no technique has however been developed to notice the pretend pictures generated by generative image editing techniques. If these images are examined by humans,

the cost increases drastically as the number of to-be-examined images increases. Obviously, detection via human eyes is insufficient for the big data era. On the other hand, conventional image forgery detection techniques are designed with different assumptions that may not be appropriate for generative fake image detection. Therefore, generative fake image detection demands specific studies and Designs.

II. Literature Survey

Akhilesh Kumar Yadav [11] introduced a method for detecting copy-move forgery which is one of the difficult types of forgery. This method is good at some manipulation/attack like JPEG compression, rotation, Gaussian noise, smoothing, scaling etc. The image is partitioned into blocks and exact matches are made between patterns of different blocks and then results are calculated using Discrete. Wavelet Transform (DWT).

Yongzhen Kel, Qiang Zhang [12], in this paper, a detection method is proposed to effectively locate image forgeries by detecting inconsistency of image noise variance on the saturation component of HSV color space. The image is first converted to HSV color space from RGB color space. Then, the images were divided into blocks of different sizes and 100 forged images were randomly cropped at different locations from the images for each size and white Gaussian noise was added. The evaluation results demonstrate that the noise estimation for image blocks with size of 32×32 achieve the best results. However the drawback was that the noise estimation for 16x16 and 64x64 pixels images was poor.

Vijay Anand [13] proposed dyadic wavelet transform (DyWT) in Combination with scale invariant feature transform (SIFT) to detect copy-move forgery. Firstly, DyWT is applied on the given test image which decomposes the image into four sub-bands LL, LH, HL, HH. Then, to extract the features of the image SIFT is applied on the LL part only as it contains the maximum information. Using these key features the descriptor vector is obtained and Similarities are find out between them in order to find the tampered region on the given image. The drawback of this method is that it is not robust to the angles defining the camera axis orientations for image.

Jian Wu [14] has provided a comparative and systematic analysis of SIFT and its family, including PCA-SIFT, GSIFT, CSIFT, SURF and ASIFT. The Performance is measured and time consumption is calculated in different Situations. The results concluded that each algorithm has its own advantages.

Nirupma Tiwari [15] proposed a method for tampering detection in which the original image is divided into overlapping blocks and for each block number of connected components are calculated. By calculating the difference between vectors of the original and tampered image the location of tampering is detected and measured. However the drawback of this method is that it is applicable on similar sized square images only. In future it can be extended to different sized images

Sai Prasanthi [9] describes an approach for verification of Indian currency banknotes. The currency will be verified by image processing techniques. In this article, six characteristic features are extracted. The approach consists of a number of components including image processing, edge detection, image segmentation, characteristic extraction, comparing images. The characteristics extraction is performed on the image of the currency and it is compared with the characteristics of the genuine currency. The Sobel operator with gradient magnitude is used for characteristic extraction. Paper currency recognition with good accuracy and high processing speed has great importance for banking system. [Sobel operator or Sobel filter is used in image processing and computer vision, particularly within edge detection algorithms where it creates an image emphasizing edges]

Komal vora [10] suggests a widespread review of study on paper currency recognition system. A number of techniques applied by a diversity of researchers are proposed briefly in organize to evaluate the condition of art. Here, the author focuses primarily on currency detection system including different steps like image acquisition, feature extraction and categorization system uses different algorithm. The classification result facilitates the recognition of fake currency mainly using serial number extraction by implementing optical character recognition (OCR). It is found that the proposed method gives superior results.

III. Existing Systems

FCID-HIST Histogram Based Fake Color Image Detection

The existing differences, we Histogram based Fake Colorized Image Detection (FCIDHIST) method to detect fake colorized images.the saturation feature Fs, the dark channel feature Fdc and the bright channel feature Fbc, are proposed to detect forgeries. The hue feature is built from the normalized hue channel histogram distributions. Let Kh be the total number of bins in every normalized hue channel bar graph distribution. We define Dist h , n and Disth h,f as the normalized hue channel histogram distribution for the natural and fake training images, respectively, and Disth as the corresponding histogram for the αth input image, which may be either a coaching or testing image.

The natural pictures, the distinctive features should reveal the largest divergences between the two types of images. (Note that the Euclidean distance is employed in this paper to calculate the divergences.) Therefore, we select the most distinctive bin Dist h (υh), whose two corresponding bins in Dist h;n and Disth h,f give the largest divergence between the two histogram distributions, as part of the hue feature.

FCID-FE Feature Encoding Based Fake Image Detection

FCID-HIST gives a decent performance in the Experiments, which are demonstrated in the latter section, these options might not totally utilize the applied mathematics variations between the natural and pretend colorized pictures as a result of the distributions are modeled channel by channel.

Therefore, we have a tendency to propose another theme, Feature secret writing primarily based faux Colorized Image Detection (FCID-FE), to higher exploit the applied mathematics data by put together modeling the info distribution and exploiting the divergences within totally different moments of the distribution**.**

IV. PROPOSED System Architecture

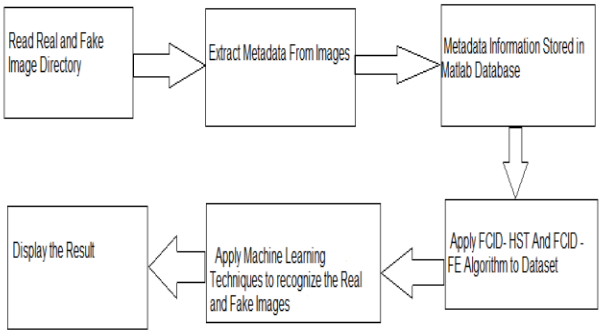

Fig. 1 Architecture of the system

V. Algorithm of System

1. Read Directory of of Fake and Real Images
2. Extract Metadata of Real and Fake Images
3. Apply FCID –HST with Machine Learning
4. Apply FCID –FE with Machine Learning
5. Compare the Results
6. Display the Results

Steps for implementation

We will Add Machine Learning Techniques to Above Algorithms The process of machine learning is similar to that of data mining. Both systems search through knowledge to seem for patterns. However, rather than extracting information for human comprehension as is that the case in data processing applications machine learning uses that information to notice patterns in information and regulate program actions accordingly. Machine learning algorithms square measure typically classified as being supervised or unsupervised. Supervised algorithms will apply what has been learned within the past to new knowledge. Unsupervised algorithms can draw inferences from datasets.

Facebook's News Feed uses machine learning to personalize each member's feed. If a member frequently stops Scrolling so as to browse or "like" a selected friend's posts, the News Feed will start to show more of that friend's activity earlier in the feed. Behind the scenes, the software is using statistical analysis and predictive analytics to identify patterns in the user's knowledge and use to patterns to populate the News Feed. They observe the activities of the user like, comment, share etc on numerous posts and supported these activities the contents on the news feed are adjusted endlessly.

VI. Results

Naive Bayes Classification: Naive Bayes classifiers are a family of simple probabilistic classifiers based on applying Bayes' theorem with strong (naive) independence assumptions between the features. The featured image is the equation—with P(A|B) is posterior probability, P(B|A) is likely hood, P(A) is class prior probability, and P(B) is predictor prior probability.
Some of real world examples are:

- To mark an email as spam or not spam
- Classify a news article about technology, politics, or sports.
- Check a piece of text expressing positive emotions, or negative emotions?
- Used for face recognition software.

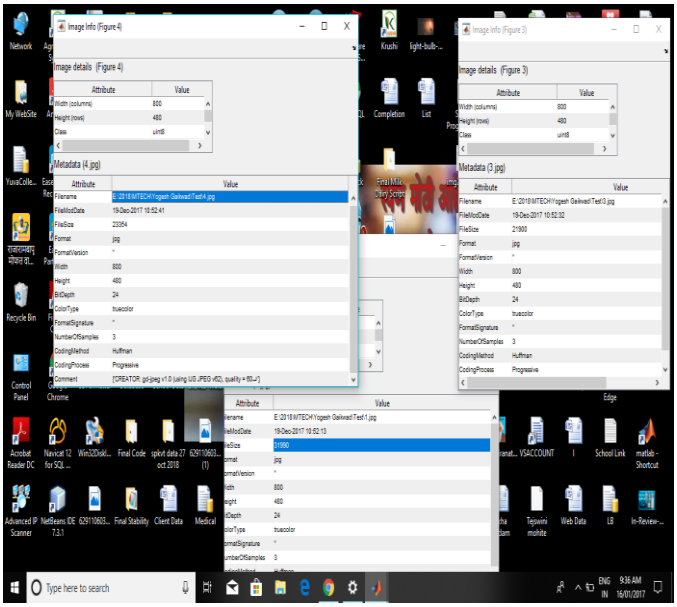

Fig 2 Extraction of Metadata

Attribute	Value
Width(Columns)	800
Height(Columns)	480
Class	uint
Image Type	truecolor
File Mod Date	19 DEC 2017 10:52:41
FileSize	233354
Format	jpg
FormatVersion	‘‘
Width	800
Height	480
BitDepth	24
ColorType	truecolor
FormatSignature	‘‘
Number of Samples	3
Histogram	

VII. Possible Outcomes

As We Passes the two dataset for the system so outcome is to distinguish the images as the real and fake Images

VIII. Mathematical Model

Precision and Recall correspond to exactness and completeness of the results. In our perspective, the Precision is applied to estimate the probability that a detected regions correct.

$$P = \frac{|I_I \cap I_D|}{|I_D|} \times 100\%$$

This probability is defined as follows: where II and ID denote the in painted region and detected region, respectively. The operator counts the number of pixels in the region**,** Alternatively, Recall is used to measure the probability that a corrected region is detected.

IX. Conclusion

Fake colorized image detection. We Observed that fake colorized images and their corresponding natural images possess statistical differences in the hue, saturation, dark and bright channels. We planned 2 easy nonetheless effective schemes, FCID-HIST and FCID-FE, to resolve this detection downside.

FCID-HIST exploits the most distinctive bins and total variations of the normalized histogram distributions and creates features for detection, while FCID-FE models the data samples with GMM and creates Fisher vectors for better utilizing the statistical differences. We evaluate the performances of the proposed methods by selecting parameters for FCID-HIST and FCID-FE and detecting different fake images generated by state-of-the-art colorization approaches.

The results demonstrate that both FCID-HIST and FCID-FE perform decently against different colorization approaches and FCID-FE provides more consistent and superior performances compared to FCID-HIST in most of the tests. Although the proposed FCID-HIST and FCID-FE give decent performances in the experiments, this paper is only a preliminary investigation, and there are many directions for future studies that require further exploration. so we need add the Machine Learning technique.

By Using Two Dataset one for fake and one for real Images we can conclude the fake and real images depends upon machine Learning Techniques.

X. 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] 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.

[9] B.Sai Prasanthi, D. Rajesh Setty , Indian Paper Currency Authentication System using Image processing International

Journal of Scientific Research Engineering & Technology (IJSRET), ISSN 2278 – 0882.

[10] Komal Vora, Ami Shah, Jay Mehta, A Review Paper on Currency Recognition System, International Journal of Computer Applications (0975 – 8887) Volume 115 – No. 20, April 2015.

[11] Akhilesh Kumar Yadav,' Forgery (Copy-Move) Detection In Digital Images Using Block Method', International Journal of Collaborative Research in Engineering Sciences(2348-9707) Volume I Issue 2, April, 2014

[12] Y. Ke1, Q. Zhang, W. Min and S. Zhang, "Detecting Image Forgery Based on Noise Estimation", International Journal of Multimedia and Ubiquitous Engineering, vol. 9, no. 1, (2014), pp. 325-336

[13] Mohammad Farukh Hashmia , Vijay Anandb ,' Copy-move Image Forgery Detection Using an Efficient and Robust Method Combining Un-decimated Wavelet Transform and Scale Invariant Feature Transform', 2212-6716 © 2014 The Authors. Published by Elsevier B. V. AASRI Procedia 9 (2014) 84 – 91.

[14] Jian Wu,' A Comparative Study of SIFT and its Variants', Measurement Science Review, Volume 13, No. 3, 2013.

[15] Nirupama Tiwari,' Reducing Forged Features Using Tampered and Inconsistent Image Detection Techniques in Digital Image Processing, Fifth International Conference on Communication Systems and Network Technologies (CSNT), DOI: 10.1109/CSNT.2015.286 Conference: 2015

I.

,