Enriching Fake Colorized Image Detection

[1]Neetu Pillai, [2]Dr.Ashok Kanthe, [3]Srijita Bhattacharjee
[1,2,3]Department of Computer Engineering, Pillai HOC College of Engineering and Technology, Maharashtra, India

Received: March 05, 2019 Accepted: April 07, 2019

ABSTRACT: : *As the social media grows, the use of the fake images are at their highest, more than 50% of the images stored at the data centers or in the cloud are being morphed or fake. So, this eventually increases the risk of storage and also processing complexity of the images. Very few systems exists to tell whether images are fake or not with not so great accuracy. The Neural network being the most advanced of all, identifies fake images by using different features of the images and by using the learning process of the pattern of faking an image. Proposed methodology uses features like Hue, alpha channel and RGB channel. Edges are evaluated using the Gaussian distribution to identify the features of the fake colorized images. Convolution neural network perform deep forensic analysis along with the fuzzy classification process to enhance the probability of identifying fake images.*

Key Words: *Gaussian Distribution model, Image Features, Convolution neural network.*

I.INTRODUCTION

People say that a picture is worth a thousand words, which holds truer than ever, owing to the digital age and the enormous influx of cameras and Smartphone that are equipped with the latest sensor hardware. These factors contribute to an exponential growth in the number of photographs. As the number of images keeps increasing, there is also an influx of an almost equal number of forged images. We live in an age where anything can be altered or manipulated with assistance from technology. The forged images are designed with nefarious purposes to discredit the original owner by persons with malicious intents.

Due to a large number of forged images, it is necessary to be able to discern an original image from the forged ones. The researchers infer that the two most widely used techniques of forgery are Copy-Move forgery and Image Splicing. The copy-move method is more common in comparison to the Image splicing technique. With the introduction of innovative image editing applications such as Photoshop, GIMP etc. the process of forgery has been simplified and introduce modifications discreetly. Therefore, the discovery of forged images is paramount to maintain the integrity and authenticity of the original image.

Machine Learning imitates human-like response, this is necessary for certain applications where reasoning is heavily required for the process to be completed. This is usually achieved with the help of certain computational networks known as neural networks. Machine learning could be fed data about the types of image forgery techniques, as it learns, with every picture, the algorithm gets faster and a lot more accurate. Once the relationship in-between all the system components is completely established, the machine learning algorithm is stopped. Its addition into the forged image detection can be very useful as a machine would not be biased and a person cannot go through a large set of images efficiently. Machine learning can help identify the patterns in the image to verify its validity. Application of machine learning into the image forgery speeds up the process and generally out-performs most of the conventional methods.

Colorization of grayscale images is not a complex task for the creative human brain. A person is only required to recall that grass is green and the sky is blue, for various other objects, the mind is free to imagine several possible colors. Deep CNN can assist as tools to consolidate localization and semantic parsing into a colorization system. The researchers have done an extensive study on the image forgery techniques and their detections and provide us with an exhaustive evaluation of the detection methods utilized in determining the type of forgery, copy-move, re-sampling, splicing, retouching etc. For the purpose of identification of fake images, it is imperative that we look for the sources of the

II.LITERATURE REVIEW

J. Li[1] introduces a method of the image with CMF consists of no less than a few areas in which contents are indistinguishable. CMF maybe conducted by a forger pursuing to enhance the visual effect of the image or to cover the truth. In this light, the researchers propose to segment the test image into a number of non-overlapped patches. Therefore, by coinciding these patches CMFD can be executed , as long

as the copying source regions and the pasting target does not exist in the same patch. This paper mainly focuses on the detection of the segment copied from one image into another image for the purpose of faking an image. Here a source image is needed to identify the forgery. This paper proposed a CMFD strategy established on image segmentation. The proposed method is very computationally taxing and could be done in a better way with the integration of parallel processing.

G. Larsson[2] narrates about Colorization of grayscale images. The technique of automatic colorization transforms two impulsive observations into a design philosophy. Firstly, semantic information matters. In order to colorize random images, a system must perceive the semantic configuration of the scene in addition to localizing objects. Deep CNNs can assist as tools to consolidate localization and semantic parsing into a colorization system. The article presents a system that demonstrates the conventional ability to automatically color grayscale images. Two innovative offerings enable this development: a color histogram prediction framework and a deep neural architecture that is trained to integrate semantically significant features of diverse complexity into colorization.

M.A. Qureshi[3] explores the advent of digital images and their proliferation in this new internet age. The extensive use of smartphones and cameras has led to an abundance of images which in turn has increased the probability of persons with mischievous intents to tamper and forge images by leaving very little or no trace. The researchers have done an extensive study on the image forgery techniques and their detections and provide us with an exhaustive evaluation of the detection methods utilized in determining the type of forgery, copy-move, resampling, splicing, retouching etc. The researchers after having done an extensive evaluation of the techniques have come across an observation that the researchers who have been actively developing methods and algorithms for tampering detection have not been paying attention to the research that goes into counter-forensics or anti-forensics. This area of research focuses on the explicit removal of tampering traces been sought after by these forgery detection methods.

D. Gragnaniello [4] explains that due to the inflation of social media as it turns into a quite powerful communication tool. Due to the boom of social media, there has been an enormous influx of manipulated images. This has led to an epidemic and there are researchers that have been trying to combat this problem with the inclusion of CNN's in their detectors. As recent studies have shown that CNN based detection methods are vulnerable to attacks. Therefore, to ameliorate this effect the researchers have analyzed the adversarial attacks done on various different CNN based detection systems and tested their performance adequately. The study concentrates only on the attacks that take place on a CNN based network, which is very limiting and have not proposed any remedial systems that can be used in the absence of a CNN based approach.

Y. Guo [5] introduces the different types of forgeries that can be done on an image and the various ways that can be used to detect the fakes. But this does not take into account the colorization of grayscale images. This is difficult to detect as there aren't many techniques that have been developed for the detection of fake colorization of the images. Therefore, to detect fake colorized image the authors proposed two different methods, the first one is the FCID-HIST Histogram based Fake Colorized Image Detection, and the other one is the FCID-FE which stands for Feature Encoding based Fake Colorized Image Detection. These techniques have been proven to be better than the traditional detection methods by a big margin. As with any learning method, most of the detection depends on the kind of training given to the system and is limited by that perspective, as it cannot detect forgery even when the image is forged, but the system is limited to its understanding.

III.PROPOSED METHODOLOGY

The proposed idea of finding fake colorized images is depicted in the below proposed methodology figure 1. And the steps involved in this process are elaborated deeply with the below mentioned steps.

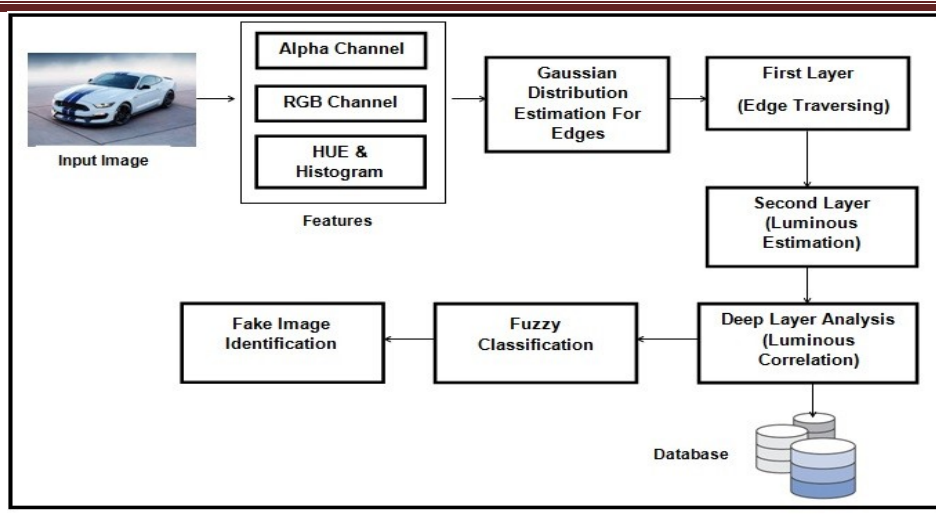

Figure 1: Over view of the Proposed Idea

Step 1: Feature Extraction - This is the very first and very important step of the proposed model. Here the base features are like Hue, alpha channel and RGB values are extracted from the input image and process in a list.

To fetch these features proposed system take input to traverse each and every pixel to get a signed integer ($P_{SIGN)}$. Then on right shifting 24 bits and then AND one hexadecimal value yields Alpha channel value. Right shifting 16,8 and 0 bits and then AND one hexadecimal value yields the Red, Green and blue channels respectively. This can be shown in the equation (1,2,3,4)

$\alpha = P_{SIGN >>} 24$ AND HEX _____(1)

$R = P_{SIGN >>} 16$ AND HEX _____(2)

$G = P_{SIGN >>} 8$ AND HEX _____(3)

$B = P_{SIGN >>} 0$ AND HEX _____(4)

Where
P_{SIGN} - A Singed Integer
HEX -Hexadecimal Number

Hue Feature- It indicates the frequency of the light that eventually is represented by a single variable. Hue can be estimated using the ratio of difference between the other two colors for maximum of RGB to the difference between max and min.

Histogram feature - The image Intensity is adjusted based on the histogram of the pixels, which can be evaluated using the equation 5.

P_N=No of pixels with intensity n / Total no of Pixels __ (5)

Where
P_N - Image with N pixels

Step 2: Edge Estimation - If an image is morphed or colorized, then the edges of the objects in the image are always tend behave out of the natural values. These edges are eventually helping us to identify the border area of the objects in the image.

Edge Detection is used for this purpose, which works based on the 5 following steps.
i) Smoothing - Here image is blurred using the Gaussian blur technique to widen the edges of the objects in the image. For this Gaussian distribution technique is used as shown in equation no 6.

ii) Finding the gradients- Here the edges with the maximum width is identified.
iii) Non- maximum Suppression - Edges with the maximum width is labeled.
iv) Double Thresholding - Here the edges which are already labeled are doubled by their width.
v) Edge Tracking- Here all the threshold edges are traversed recursively to mark them in white color and rests of the pixels are marked with the black color.

$$f(x \mid \mu\ \sigma = \frac{1}{\sigma \quad \pi} \cdot \frac{x-}{2\sigma} \quad \text{\_\_\_\_\_ (6)}$$

Where μ is mean, x_i instance pixel value,δ is the Standard deviation

Step 3: First Layer of the CNN (Edge Traversing) **-** Here this is the first layer of CNN wherethe edge image is taken into consideration to traverse on only edges and record their luminance with respect to the orignal image. This is because if the image is natural then the luminance of the image is undisturbed by the external colors. If it is edited or morphed to create its fake version, then it is disturbed in many locations. This process can be depicted in below algorithm.

ALGORITHM: Edge Traversing

// Input: Edge Image $I_{E,}$ Original Image O_I
// Output: Pixel List P_L
//T_L : Temporary List
// I_{SIGN}: Signed Integer
1: Start
2: **For** i = 0 to size of Width of I_E
3: **For** j=0 to size of Height of I_E
4: $I_{SIGN} = I_{E(ij)}$ RGB
5: R= I_{SIGN} >> 16 & H_D
6: G= I_{SIGN} >> 8 & H_D
7: B= I_{SIGN} >> 0 & H_D
8: **IF**(R==255 && G==255 && B==255),THEN
9: $L_U \rightarrow$luminance(R_{OI},G_{OI},B_{OI})
10: $T_L \rightarrow$ I,J,L_U
11: ADD T_L to P_L
12: End IF
13 :**End for**
14:**End for**
15: **return** P_L
16: Stop

Step 4: Second Layer of the CNN (Edge Traversing) - Here in this step once the Edge image pixel position for white pixel is recorded as I,J. then, with respect to this I and J RGB of the original image is extracted to evaluate the luminance based on the equation no 6.

Luminance= 0.299 * R + 0.587 * G + 0.114* B ____(7)

Luminance is the component that represents the amount of white light on the pixel, For any natural image luminance of the edges of the images are always remain intact. For any forgery in the image , luminance keep changing on the edges.

Step 5: Third Layer of the CNN (Luminance Correlation) **-** Here in this step a correlation array is created in the edge pixels based on the values of luminance and the histogram. Then another correlation array is created with respect to the trained images stored in the database for the luminance and histogram.

Then these two arrays are fed to Pearson correlation estimation technique, which eventually generates a decimal value in between the 0 and 1 as shown in equation 8. This correlation value is subjected to classify the image into fake or original based on the Fuzzy classification model.

$$r = \frac{\sum xy - \frac{\sum x \sum y}{n}}{\sqrt{(x^2 - \frac{\sum x^2}{n})}\sqrt{(y^2 - \frac{\sum y^2}{n})}} \quad \text{_____(8)}$$

Where
x is the entities of Query image
y is the entities of trained images from database
n is the array Size

Step 6: Fuzzy Classification- Here in this step a correlation array result which is in the range of 0 to 1 is divided into 5 parts with respect to the Fuzzy crisp values. Fuzzy Crisp values are VERY LOW, LOW, MEDIUM , HIGH AND VERY HIGH.

A fuzzyfier engine is used to classify the value for the fake or original based on the classification label of crisp values. Any value which is nearer to 1 is rated as thevery highly fake . Where as the any value which is nearer to 0 is rated as non fake or original.

IV. RESULTS AND DISCUSSIONS

In this section the proposed system of fake image detection using the features like histogram and CNN, which is boosted using fuzzy classification is subjected to some experiments to evaluate its performance with comparison of same existed methodology. The proposed model is deployed in real time scenario using Java programming language and Netbeans as the IDE in Core i5 Environment with the primary memory of 6GB.

Histogram Equalization Result (HTER)-Proposed model is put under hammer for HTER with the comparison of the two different methods are used to identify the fake colorized images as FCID-HIST and FCID - FE[5].

FCID-HIST: Here in this step four features are being extracted from the images like Hue, Saturation, Dark Channel, and Bright Channel. Once these features are being extracted, then they are aggregated to normalize the histogram. And then the proposed methodology deploys the features into Support vector machine (SVM) to get the classification values which are being used to classify the fake colored images.

FCID - FE: Here in this step again four features are being extracted as mentioned in FCID-HIST and then these features are subject to identify the distribution of data using Gaussian mixture model and exploring the divergence inside the different moments of the distribution. And finally Gaussian mixture model is blended with the SVM training Classifier. Where LIBSVM Classification protocol is being used to identify the Fake images.

Cross Validations are performed on the basis of histogram role to identify the fake images on FCID-HIST, FCID-FE of [5] and with the proposed model of FCID- CNN on various image folders belong different categories like sports, nature, sky etc. The table 1 represents the cross validation result between the FCID-HIST, FCID -FE and FCID-CNN.

Table 1 : HTER Results of Cross Validation in Percentage

Folder No	FCID - HIST	FCID-FE	FCID-CNN
1	21.8	16.65	14.5
2	22.9	16.9	14.5
3	21.7	16.65	14.5
4	15.2	16.9	14.3
5	16.8	16.9	14.2
6	16.65	17.21	14.5
7	17.78	16.84	14.5
8	17.59	17.24	14.7
9	16.98	16.89	14.5
10	16.84	16.98	14.5

On observing the values and the plot in figure 2 and 3 it clearly indicates the fact that FCID -CNN provides better performance than that of FCID-HIST and FCID-FE. Where average HTER of FCID -HIST is around 18.423%, Average HTER of FCID-FE is around 16.994 % and average FCID-CCN is about 14.47%.

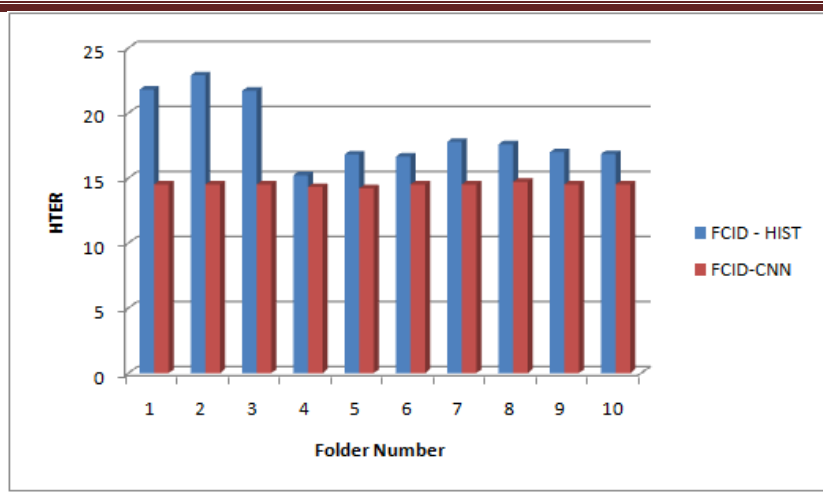

Figure 2: HTER Comparisons of Cross Validation between FCID- HIST and FCID-CNN

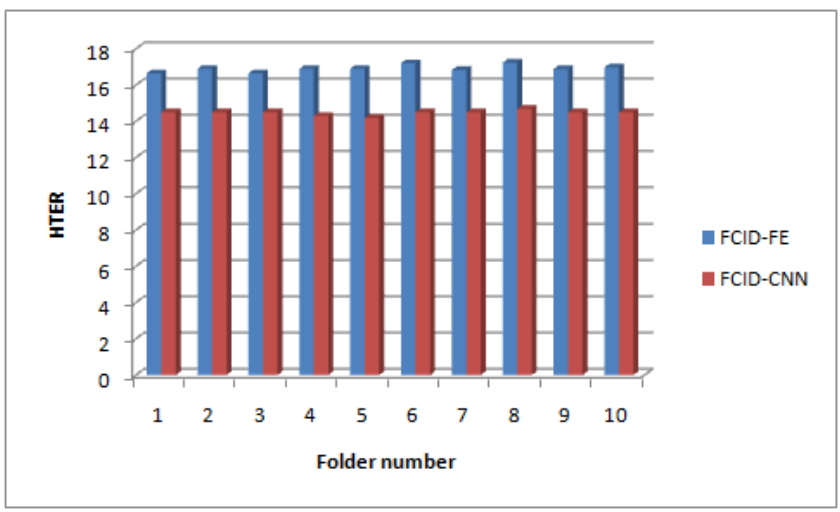

Figure 3: HTER Comparisons of Cross Validation between FCID- FE and FCID-CNN

On observing some facts on FCID-HIST in [5] it indicates that the using SVM for all different types of images creates different bins of distinctive values so it is not performing well than that of FCID-FE. On the other hand FCID-FE out performs than that of FCID-HIST because of the moments based feature extraction using Gaussian mixture model. But on the other side FCID-CNN shows more improved results than that of FCID-FE due to using of Gaussian kernel model and CNN, which enhances the process with better average result of 14.47%.

V. CONCLUSION

This research paper properly scrutinizes the different features of the images like hue, saturation, dark channel, bright channel and an alpha channel. Then Distribution factors of all these features are being estimated using a Gaussian distribution model for the edges of the images, which indeed the plays a vital role in identifying morphed and fake colorized images.

Then based on this distribution factor the convolution neural network efficiently handles the fake image detection process based on the luminance factor of the image edges. The Correlation between the luminance of the real edges and the fake edges are being estimated using Pearson correlation model. To efficiently classify the Pearson correlation fuzzy classification model is being used to enrich the model.

The Histogram equalization results are being evaluated in between FCID-FE and FCID-HIST of [5], where the proposed model's concept of FCID- CNN performs better by 4% compared to FCID-HIST and 2.5% compared to FCID_FE. In the future this fake image detection process can be enhanced to more accurately by considering more vigorous features like DCT and wavelet transform techniques to handle more deep High definition images of space and etc.

VI. REFERENCES

1. J. Li, X. Li, B. Yang,and X. Sun, "Segmentation-Based Image Copy-MoveForgery Detection Scheme," IEEE Trans. Inf. Forensics and Security, vol.10, no. 3, pp. 507-518, 2015.
2. G. Larsson, M. Maire,and G. Shakhnarovich, "Learning representations for automatic colorization," in Proc. European Conf. Comp. Vision (ECCV), pp. 577-593, 2016.
3. M.A. Qureshi and M. Deriche, "A bibliography of pixel-based blind image forgery detection techniques," Signal Process.: Image Communication,vol. 39, pp. 46-74, 2015.
4. Diego Gragnaniello, Francesco Marra, Giovanni Poggi, Luisa Verdoliva, "Analysis of Adversarial Attacks against CNN-based Image Forgery Detectors", 26th European Signal Processing Conference. 2018.
5. Y. Guo, X. Cao, W. Zhang,and Rui Wang, "Fake Colorized Image Detection", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, 2018
6. Y. Zhao, X. Zhang, M. Xu, Z. Sun and G. Liu, "Web Identification Image Recognition Based on Deep Learning", 3rd International Conference on Information Science and Control Engineering, 2018.
7. M. Bachtiar, D. Gusti, M. Hidajat and I. Wijaya, "Web-Based Application Development for False Images Detection for Multi Images Through Demosaicing Detection", International Conference on Information Management and Technology, 2018.
8. Tushar D. Gadhiya, Anil K. Roy, Suman K. Mitra,and Vinod Mall, "Use of Discrete Wavelet Transform Method for Detection and Localization of Tampering in a Digital Medical Image", IEEE Region 10 Symposium, 2017.