Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 09, September-2020

Adaptive and Improved Approach for Image Forgery Detection

Raneem Tassia
Faculty of Information Technology
Syrian Virtual University
Lattakia, Syria

Dr. Mohamad-Bassam Kurdy
Faculty of Information Technology
Syrian Virtual University
Damascus, Syria

Abstract: **The study presented through this research deals with the subject of digital images. "An image is worth a thousand words" and is considered more powerful and reliable as evidence because it is used in many fields and applications that impact multiple aspects of our life. The purpose of this research is to detect forgery that can be applied to digital images, which aims at masking the truth by providing false and incorrect information, causing problems, especially in critical areas such as health applications and criminal investigations. The proposed system provides an adaptive and dynamic application, which can detect the two most common and most used types of forgery: Splicing forgery and Cloning (copy-move) forgery. This system can detect the two types of forgery in different types and sizes of images, unlike many previous studies that concentrated on a specific type of forgery, or an image with specific characteristics and conditions. The application dynamically adapts to the given image and selects the optimal algorithm that fits said image, to arrive at the best result in detecting the forgery based on the image's data and specifications. The proposed system also reduces the number of false alarms (false positives) generated by the basic systems which the application relies on when detecting Cloning forgery. The two basic systems presented in previous studies suffered from a large number of false positives that suggested the existence of fraud although the original image was not forged. Therefore, one of the aims of this study was to both identify and handle the causes of these false positives in each method separately thereby improving on the performance of the original algorithms.**

Keywords: Image forgery; cloning; splicing

I. INTRODUCTION

It is impossible to imagine our life without images. Unfortunately, there are several image processing software that are available and accessible to everyone, which can be easily used to change the content of an image without even leaving any visible trace of the processing operation. Therefore, because people generally believe what they see, there is an important and urgent need to develop image forgery-detection systems, which are capable of verifying the authenticity and reliability of images.

Image forgery is defined as the process that changes the original image by adding some parts or properties, or changing or even deleting them in an invisible manner [1]. There are three classifications of digital image forgery: Copy-move forgery, Image splicing, and Image re-sampling. A brief explanation of each will be provided in the next section.

The main objective of this paper is to present an integrated framework that can detect the two most basic types of forgery, which are Splicing and Cloning. The proposed application allows for choosing the type of forgery to detect (Splicing or Cloning), can process pictures of different sizes and, selects the appropriate algorithm to detect copy-move forgery of the examined image.

II. BASIC TYPES OF IMAGE FORGERY

A. *Image Splicing*

This type combines sections from two or more images to generate a fake image as demonstrated in Fig. 1. Although this operation may not leave any trace, it disturbs some of the image statistics, which can be used in detecting forgery [2].

Fig. 1 (a, b) original images, (c) fake image

B. *Copy-Move Forgery*

In this type of forgery, some parts of an image of any size and shape are copied and pasted to another area of the same image, either to camouflage or to clone the object in the image multiple times, as demonstrated in Fig. 2. The duplicated regions have the same features because they are taken from the same source, hence it is hard to detect it [3].

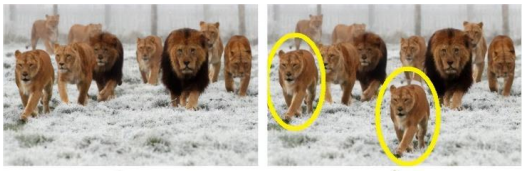

Fig. 2 (a) original image, (b) forged image

III. IMAGE FORGERY DETECTION TECHNIQUE

There are two major types of detection techniques: Active and Passive. Which technique to use depends on the original image and whether any information about it is known or not.

A. *The Active Approach*

The Active forgery detection techniques, such as digital watermarking or digital signature, use some information embedded into the original image. By verifying this code from the original image against the examined image, authenticity is proved. These techniques need special hardware or software to insert the code [4].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 09, September-2020

B. The Passive Approach

The Passive approach uses the information available in the examined image only, such as texture, color, features. There is no need to know anything about the original image thus it is also known as a blind approach. This approach uses the available features to check for image authenticity [5].

In our proposed method, the Passive approach is used to check image authenticity and genuineness, because it is more effective than the Active approach and does not need any special conditions.

IV. THE PROPOSED SYSTEM

The proposed system combines three existing methods, one for detecting Splicing forgery and, the other two for detecting Cloning forgery. The reason behind using two algorithms for detecting Cloning, is that each one of them works properly and gives good results in certain conditions related to the image itself but, breaks down in other cases. So the proposed system combines them in order to increase the ability of the application to deal and work properly no matter what the image properties are.

In addition, the proposed application adds steps to the two methods that are used to detect Cloning, in order to reduce the high rate of False Positives (FPs) generated by those methods. These steps, which will be explained later, enhance the performance and reliability of the original algorithm.

An integrated system is presented, that can detect the two most common types of tampering applied to digital images: Splicing and Cloning. It also adapts to the image and chooses the proper algorithm to apply when copy-move forgery needs to be checked, based on the image properties.

In this proposed system the targeted image, genuineness of which is to be checked, is selected first. Then, the type of forgery to detect can be chosen. To simplify the explanation of the method, it will be divided into three cases:

A. Case 1

If Splicing forgery detection is chosen, the system applies the method proposed by [6], which depends on Color Filter Array (CFA) to detect a spliced region in case it exists, because the Splicing operation measurably changes the CFA artifacts. The image is divided into sub blocks and, each block is re-interpolated with four Bayer CFA arrangements that are most commonly used in today's cameras. Then the algorithm calculates the Mean Square Error (MSE) between the input and re-interpolated block for these four patterns. If the block is not fake, then one of the MSE values will be smaller than the other three, otherwise the block may have been tampered with.

Then the CFA patterns for all the blocks are compared, in order to find and locate the region of tampering, if it exists. If the whole sub blocks have the same CFA then the image is original and no forgery is detected. Otherwise, the difference in CFA artifacts may indicate the presence of tampering and, it will be evidence that this block is coming from another image and was merged into the targeted image, hence the forgery is detected in the said block. The basic steps of this method are illustrated in the diagram in Fig.3.

B. Case 2

If Copy-Move forgery detection is chosen, then one of two methods is applied to the image. The system chooses one of them according to the size of the image, because each method works properly only for a specific size and, if applied inappropriately, cannot detect Cloning or may cause a system breakdown.

Therefore, when the image is small, the system applies the method proposed by [7]. This method uses a Discrete Cosine Transform (DCT) to detect duplicated areas. It divides the image into 8 X 8 overlapping blocks, and then calculates the DCT feature for each block. Next, it compares the extracted features to search for matching blocks, by calculating Euclidean Distance between each block and the features of the other blocks. If the distance is smaller than a particular number, which is called the Threshold, then the two blocks are considered as duplicated blocks, thus the copy-move forgery is detected in these blocks. A Threshold value of (1.6000) is used. If no matched features are found, then the image is not fake.

One drawback of this method is that it can only work for small images and, it causes a system breakdown if used with larger images, so the proposed method applies Case 3 when the image is big.

The other big drawback is that the system generates a large number of FPs when the image has homogeneous texture areas, i.e. it shows that there is a Copy-move forgery although the image is untouched. There is a need therefore, to improve the performance and minimize the FP rate. Therefore, to enhance the original approach, the proposed method calculates the Entropy of the block before considering it duplicated or copied from another block in the image. The purpose for calculating the Entropy is that the FPs appear only in the area with a homogeneous texture and, the Entropy is one of the values that are used to measure the texture of an image. In case the Entropy is smaller than a specific value (entropy < 1) then the block is almost homogeneous and is not considered as a forged block. The optimal value of the Entropy has been defined by testing the system on different images and, determining the best value of the Entropy that decreases the number of FPs appearing in the original method. This additional step, that has been added to the original method, reduces the FPs and, at the same time, does not affect the True positives rate. The improved result will be presented later in this paper. The basic steps of this algorithm are illustrated in the diagram in Fig.4.

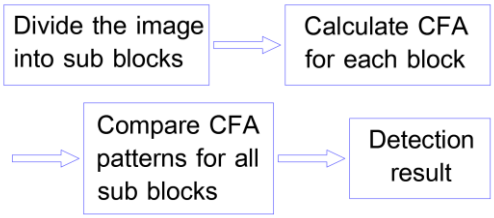

Fig. 3 Case 1 Diagram

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 09, September-2020

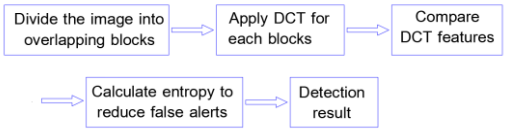

Fig. 4 Case 2 Diagram

Case 3

When the image is big, the previous method does not work. Therefore, our adopted system applies the method proposed by [8]. This method depends on the Speed Up Robust Feature (SURF) algorithm to extract features, along with a K-Dimensional Tree to define the duplicated points. The SURF algorithm defines the key points (points of interest), and then extracts a feature vector for each point. Next, comes the matching of the feature levels which uses the K-Dimensional Tree to choose the nearest neighbor for each point. If the distance between each point and its nearest neighbor is smaller than a static threshold (0.0450), then it is considered a duplicated point, thus Cloning is detected in the areas around these matching points.

This method cannot detect the Cloning forgery of small images; moreover; it has a high FP rate because it uses a static threshold. Consequently, in our method, an improvement is achieved by using a dynamic threshold. Our proposed system defines the proper threshold for each image depending on the image texture and size, which affects the number of extracted SURF points. The proposed system defines three Thresholds instead of one static Threshold used in the original approach. These values are (0.0150, 0.0100, and 0.0099), depending on the size of the image and the number of the key points. The threshold value is inversely proportional to the number of key points extracted from the image. This dynamic Threshold decreases the number of the FPs that the original system was suffering from. The improved result will be illustrated later in this paper. The basic steps of this algorithm are illustrated in the diagram in Fig. 5.

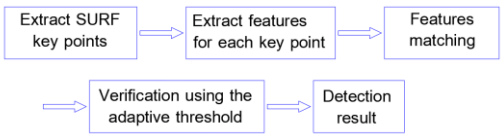

Fig. 5 Case 3 Diagram

V. TESTS AND RESULTS

The application of our methods is implemented using MATLAB R2019a. To test the result, two data sets were chosen, which are widely used in image processing research: CASIA1 and, Columbia Uncompressed Image Splicing Detection. In addition, 50 large original images were loaded from the web to test the algorithm that detects the Cloning in

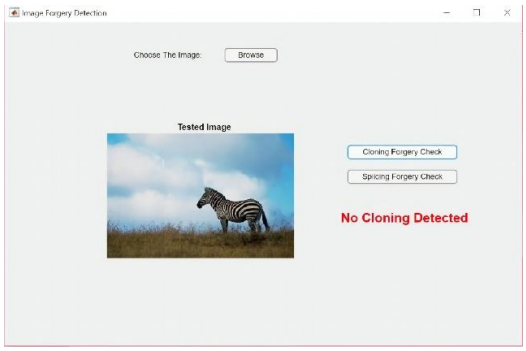

Fig. 6 Application Main Interface

big images. Fig. 6 shows the application's main interface that allows the user to choose an image, then two possibilities are available for the detection: Splicing or Cloning Detection. If the image is original (not fake) the application shows a phrase stating it is an original.

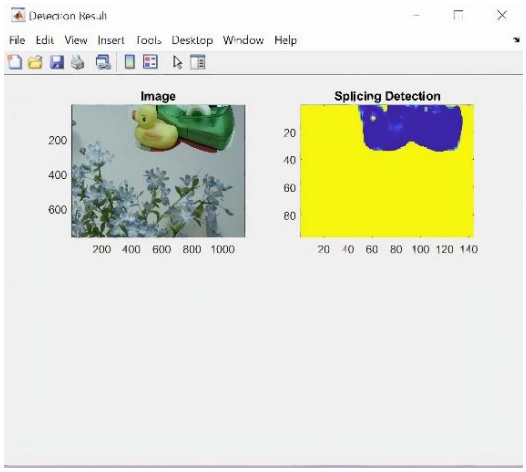

Fig. 7 Splicing detection result

If the user wants to check Splicing forgery, the application shows the result (if forgery detected) as shown in Fig. 7. It shows the image, as well as the detection result beside it. The two colors blue and yellow show that the image was generated from two different images being merged.

For Cloning detection, the application automatically chooses one of the two possible methods based on image size. The detection results have been differentiated to show which method has been applied. If the first method, that uses DCT, is applied, the result will appear in red blocks referring to the duplicated areas as shown in Fig. 8.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 09, September-2020

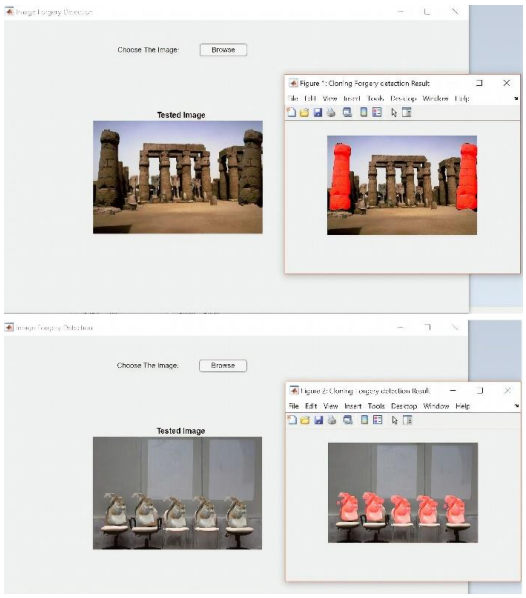

Fig. 8 Cloning detection result using method 1

Otherwise, the method that uses SURF will show the cloning using green marks in the duplicated areas as demonstrated in Fig. 9. The adaptability of the proposed system is evident where it uses and selects automatically one of two algorithms, used to detect Cloning, to apply on the image depending on its properties.

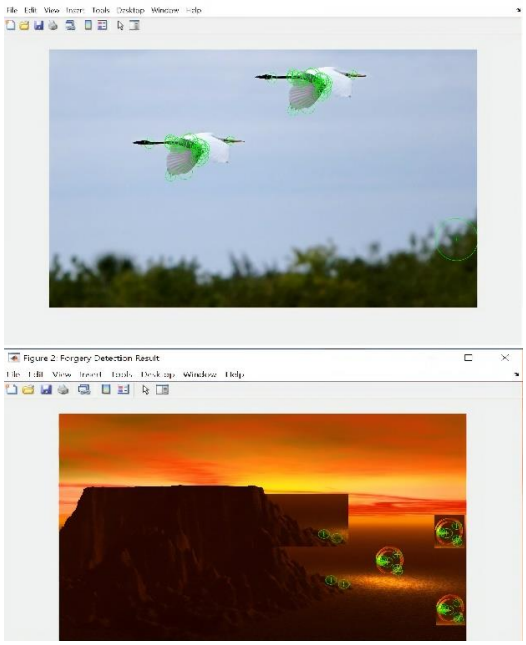

Fig. 9 Cloning detection result using method 2

VI. EVALUATION AND COMPARISON

As explained earlier in this research, the proposed method improves the performance by reducing the FP Rate in both algorithms that are used to detect Cloning forgery. In each one of them, steps are added in order to enhance the algorithm. The added steps differ from one algorithm to another.

In the first method that detects the Copy-move in small images, the proposed algorithm depends on block texture because it was realized that the FPs only appear in the homogenous areas, so the additional step that was added to the algorithm computes the entropy for each suspected block before considering it as forged. If the computed value is smaller than one, the proposed algorithm ignores it.

This additional step, which measures the texture of the blocks, by computing its Entropy, enhances the performance of the original approach by decreasing the number of FPs and, at the same time, it does not affect the detection rate of True positives.

To compare the original and the proposed method, 100 images from the CASIA1 dataset were selected and tested on both. Table 1 shows a comparison between the original algorithm and our improved one. This comparison illustrates the rate of the FPs in both methods and, shows that the FPs rate decreased significantly.

TABLE 1 COMPARISION 1

Method	False Positive Rate
[7]	0.74
Proposed Method	0.07

In the second method used for large images, the algorithm dynamically defines a proper threshold for each image depending on its properties rather than a constant threshold as per the original method. The proposed method selects one of the three possible values (0.0150, 0.0100, and 0.0099) instead of one static value (0.0450) in the original method. This dynamic selection depends on the number of the key points extracted from the image. As more key points are extracted, a corresponding lower threshold value is used, in order to minimize the number of FPs.

To compare the original and the proposed method, the 50 images that were downloaded, were modified to produce 50 additional forged images. So 100 images were used to do the tests on both of the methods.

The tests show that the number of FPs was decreased from 2300 false points in the original method, to 400 points in the proposed method. Therefore, the rate of errors decreased in the proposed method by about 83%.

The tests also show that the number of untouched images, that incorrectly show FPs, also decreased. This improved rate is shown in Table 2.

TABLE 2 COMPARISON 2

Method	False Positive Rate
[8]	0.42
Proposed Method	0.06

Also a comparison between our proposed method and the three original methods is demonstrated in Table 3. This comparison shows that the proposed system is a

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 09, September-2020

comprehensive approach that can deal with the most popular two types of forgery and, can adapt to the examined image.

TABLE 3 COMPARISON 3

Method	Splicing Detection	Cloning Detection
[7]	No	Only small images
[8]	No	Only large images
[6]	Yes	No
Proposed Method	Yes	Yes

The improved results are shown in images here. Fig. 10 shows the results of detecting Cloning in the original and proposed methods for small images (red marks show FPs). The images in the left column are the result of the original approach and, clearly they have a huge number of FPs, which shows that there is Copy-move forgery, although these images are all original and not fake. The right column illustrates the result of our proposed system after adding the additional step, that computes the Entropy and, it is obvious that we completely got rid of the FPs, which was an issue with the original system.

Fig. 11 demonstrates the improvement for large images (green marks shows the FPs). The images in the left column, which resulted from the original system, have a high number of FPs illustrated by the green marks. However, the images in the right column that resulted from our proposed system, reduce the number of these FPs. In the top image, the number is reduced from 30 FPs to approximately three FPs only, whereas in the bottom image the FPs disappeared completely.

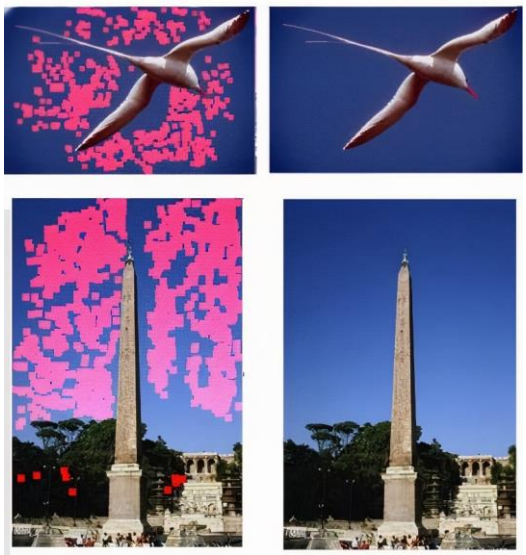

Fig. 11 left column: original method. right column: our proposed method

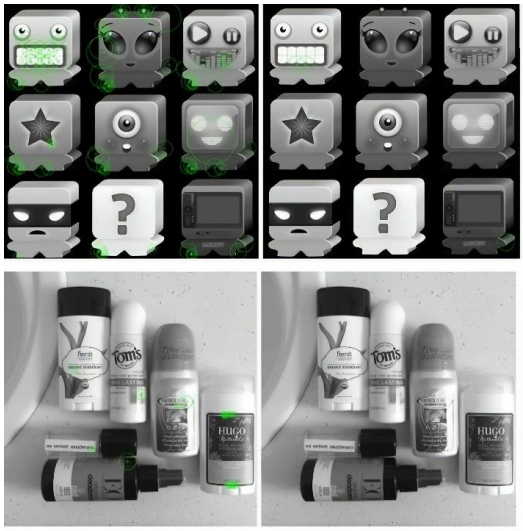

Fig. 10 left column: original method. right column: our proposed method

VII. CONCLUSION AND FUTURE WORK

This paper presents an integrated application that can detect two types of image forgery, namely Splicing and Cloning (Copy-move).

It is also an adaptive application that can deal with different types and sizes of images, by choosing automatically the appropriate method to apply to detect cloning forgery in an image. The application determines some important image parameters, and then initializes some values for optimum testing, in order to enhance the performance.

An improvement is achieved in the FP rate in both algorithms that are used for Cloning detection, by adding some steps to each one of the original algorithms; each of these added tests differ according to the original algorithm itself and, the causes of these FPs.

There are areas where future work can be done on this application. For Cloning detection, the current method is unable to detect duplicated regions in case these regions were pre-processed by resizing or rotating.

Moreover, the algorithm that detects Splicing is a general one that is aimed at detecting the global image processing such as resizing, blurring and re-compressing that are applied to the image, besides the Splicing operation. So some work can be done here to enhance the performance in an attempt to detect only the Splicing in a better and more effective manner and, to make the results more readable and understandable by the users.

It must be noted that the application is consuming a lot of time to apply the algorithm and detect the forgery, so some improvements can be done regarding complexity and processing time.

For future research, it is a good idea to search for the original image through the web, using Image Retrieval systems.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 09, September-2020

REFERENCES

[1] A. Kashyap, R.S. Parmar, M. Agrawal, H. Gupta, "An Evaluation of Digital Image Forgery Detection Approaches", 2017.

[2] M.A. Qureshi, M. Deriche, "A review on copy move image forgery detection techniques", 2014 IEEE 11th International Multi-Conference on Systems, Signals & Devices (SSD14). 2014, pp. 1-5.

[3] T. Thakur, K. Singh, A. Yadav, "Blind Approach for Digital Image Forgery Detection", International Journal of Computer Applications. 2018, pp. 34–42.

[4] G.K. Birajdar, V.H. Mankar, "Digital image forgery detection using passive techniques: A survey", Digital Investigation. 2013, pp. 226–245

[5] B.S. Kumar, S. Karthi, K. Karthika, R. Cristin, "A Systematic Study of Image Forgery Detection", Journal of computational and theoretical Nanoscience. 2018, pp. 2560–2564.

[6] A.E. Dirik, N. Memon, "Image tamper detection based on demosicing artifacts", in: 2009 16th IEEE International Conference on Image Processing (ICIP), 2009, pp. 1497–1500.

[7] N. Jadhav, S. Kharat, P. Nangare, "Copy Move Forgery Detection Using DCT", International Journal of Emerging Technologies and Engineering (IJETE) Volume. 2015, pp. 38–42.

[8] B.L. Shivakumar, S.S. Baboo, "Detection of region duplication forgery in digital images using SURF", International Journal of Computer Science Issues(IJCSI), 2011, pp.199–205.