Digital Image Forgery *

Ananga Thapaliya
Innopolis University
Innopolis, Russia
a.thapaliya@innopolis.ru

Daniel Elambo Atonge
Innopolis University
Innopolis, Russia
d.atonge@innopolis.university

Manuel Mazzara
Innopolis University
Innopolis, Russia
m.mazzara@innopolis.ru

Subham Chakraborty
Innopolis University
Innopolis, Russia
s.chakraborty@innopolis.ru

Ilya Afanasyev
Innopolis University
Innopolis, Russia
i.afanasyev@innopolis.ru

Muhammad Ahmad
University of Messina
Messina, Italy
sdistefano@unime.it

Abstract

Image control has disintegrated our trust of computerized pictures, with progressively unobtrusive fraud techniques representing a regularly expanding test to the integrity of images and their legitimacy. With the progress of advanced image controlling software and modifying tools, an electronic picture can be successively controlled. Checking the decency of pictures and recognizing indications of modifying without requiring extra pre-inserted data of the image is the basic field of inspection. In this paper, a study of such research commitments has been directed by following a well-defined and systematic procedure. There are different paths for modifying an image, for instance, copy-move, splicing, and re-sampling. This paper focuses on two types of digital image forgery detection which are copy move and splicing of image.

1 Introduction

The Digital image forensics is the procedure of modification or alteration of digital image with an arrangement to cheat other which are the precise copies of original picture [1]. The development and improvement in the field of computer

graphics have produced many photo editing software, for example Lightroom, Photoshop and many more. This alters the picture content without making any undeniable evidence of scam.

Today, these powerful images editing software enable individuals to adjust photographs and pictures easily and in a short period of time. So, it winds up troublesome for people to detect these changes and modifications. Thus, the veracity and legitimacy of digital pictures are lost. Figure 1 shows a typical example of digital image forgery. This alteration of pictures can be done for concealing some critical traces from a picture, to modify the minutiae of the picture which makes the wrong data to be transmitted. In this 21st century, there aren't any places left where digital pictures aren't utilized. They are used in pretty much every field, in particular computerized media, electronic field, financial institutions, government, military, law, industry, forensics, science and innovation, social media, fashion, medical profession and certainly everywhere throughout the web [2]. Thus, creating strategies to check the genuineness and realness of the digital images is essential, especially considering that these images are presented as a proof in a courtroom, as a piece of recuperative records or as reports which involves huge financial budgets. Hence, digital image forgery detection is one of the most important of image forensics.

Figure 1: Digital Image Forgery [9]

The aim of this work is:
1) To give a brief introduction of digital image forgery.
2) To give an outline of various types of digital image forgery.
3) To show different procedures of image forgery detection with their pros and cons

2 Types of Digital Image Forgery

Image alteration or modification is characterized as editing, that is "adding or erasing" some vital highlights from a picture without leaving any recognizable touch. There are two types of image falsifying techniques: Active and Passive approaches [3]. These types have its own specific types which is shown in Figure 2. There have been distinguished methods for falsifying a picture. Considering the techniques used for altering images there are three types of digital image forgery: Image Splicing or image composites, Copy-Move or region duplication Forgery and Image retouching.

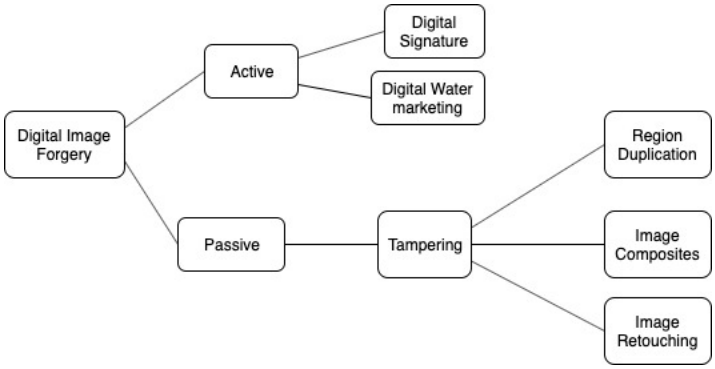

Figure 2: Types of Digital Image Forgery

2.1 Region Duplication (Copy-move forgery)

Region duplication is the most common image altering method used because of easiness and effectiveness in which image of any shape and size in specific area is reordered (copying and pasting) with another region in the same image to cover some vital information as displayed in figure 3. This is normally done so as to shroud certain subtleties or to copy certain parts of a picture [4]. The use of blur can often be seen along the fringe of modified region to lower down the inconsistencies between the original and reordered area. As the replicated part started from the same picture, its fundamental properties, for example its saturation, color and grain don't change and make the process of acknowledgment difficult. There are several attempts to detect copy-move forgery.


Figure 3: Copy-Move Forgery

2.2 Image Splicing

Image splicing is a commonly used simple forgery technique that crops and pastes regions from the same or separate sources. The splicing operation is caused by supplanting at least one parts of an image with sections of other images. There are numerous tools accessible for picture altering like enhancement, morphing and so forth [4]. Splicing is a type of photographic manipulation which involves computerized splicing of at least two pictures into a solitary composite picture which might not have further post preparing, for example, smoothing of borders among various fragments. Figure 4 is an

example of image splicing. This technique of alteration can cause irregularities in numerous features like the unusually sharp transient at the edges and these irregularities are utilized to identify the phony. Image splicing is used by advanced photograph montage with the goal that two pictures can be joined together as it is one of the most common digital image forgery practice between the well-known forgery identification methods [5].

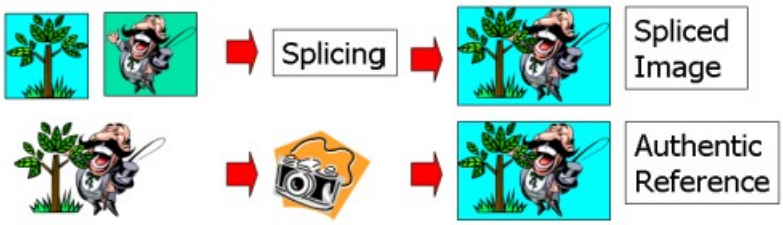

Figure 4: Image Splicing [10]

2.3 Image Retouching

Adjustment of the picture utilizing any editing software to accomplish some particular outcome, for example to ridicule others or enhance the pictures comes under this classification. This procedure does not fundamentally change a picture but rather improves or lessens the specific element of a picture [12]. To make an amazing forged picture, some chosen locales need to experience geometric changes like rotating, scaling, extending etc. The introductory step plays a vital role in retouching process and presents non-insignificant factual changes. Retouching brings explicit intermittent connections into the picture. These connections can be used to perceive forgery which is done by retouching [5]. Regardless of which camera is utilized to take pictures, it is conceivable to modify every photograph to dispose of any defects later on. Retouching involves a lot of treatments like essential shading adjustment, skin modifying, and photograph rebuilding and so on. One best case for retouching can be clarified with figure 5.

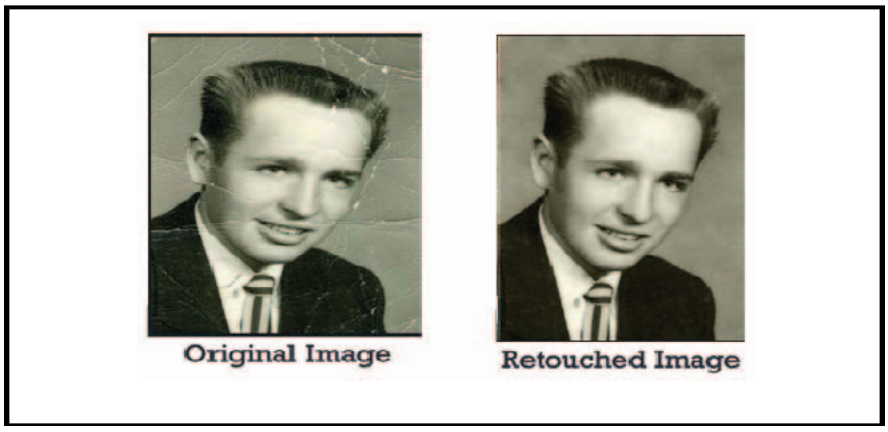

Figure 5: Image Retouching [11]

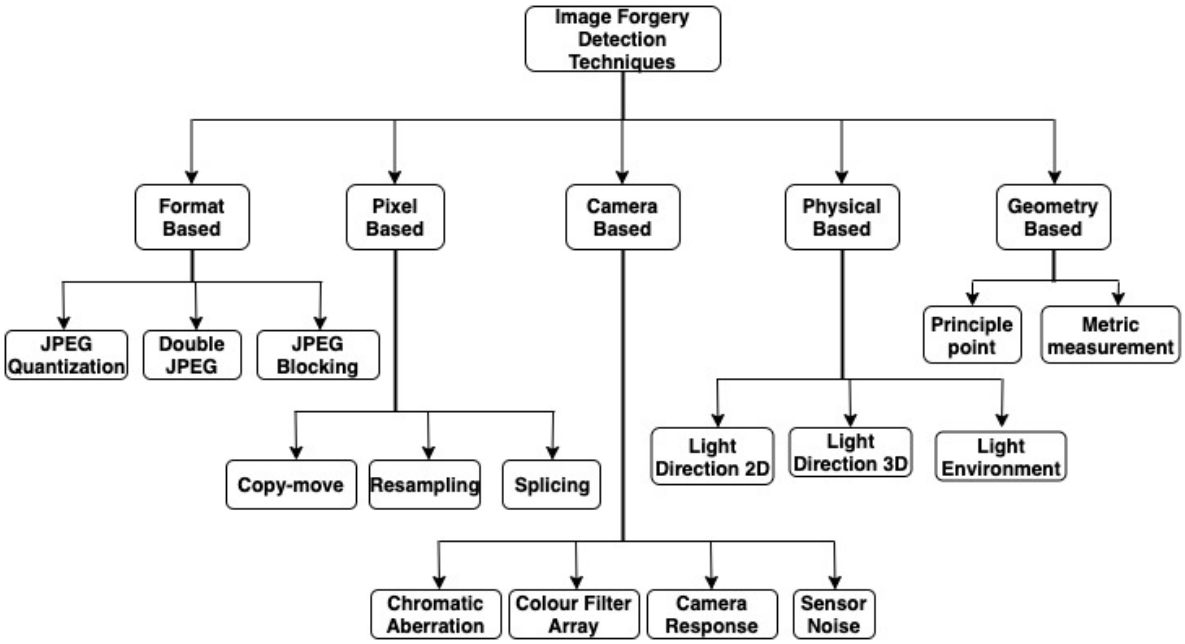

Figure 6: Digital Image Forgery Detection Techniques

3 Digital Image Forgery Detection Techniques

The undetectable phony picture detection is exceedingly refined. Any phony presents a connection among the forged picture fragments and the first section which can be utilized for effective forgery exposure. A few proficient forgery discovery methods are presented for passive digital image forgery detection which are roughly grouped into five categories. In this passive methodology, there is no pre-embedded data inside the picture amid the creation [5]. This method works simply by dissecting the binary data of a picture. Fig 6 demonstrates the different digital image forgery detection methods [6].

3.1 Format based digital image forgery detection

This method works with respect to the image format. The most preferred image on which this image forgery detection works is JPEG format. The blocking impact presented by JPEG can be utilized to identify altering in JPEG design. Manipulation of pictures causes the modification of block artifact grid, particularly in the case of preparation of copy-move [1], [2]. JPEG Quantization, JPEG blocking and double JPEG are three major classifications which can recognize picture phony also for compressed pictures.

3.2 Pixel based digital image forgery detection

This method highlights with respect to the pixels of the digital picture which are the fundamental structure blocks. These strategies take a shot at various factual abnormalities which are introduced at the pixel level. The working of these procedures depends on the adjustment's basic insights of the picture [6]. The most common detection techniques in this category are copy-move, splicing and resampling.

3.3 Camera based digital image forgery detection

When we snap a photo from a digital camera, the image moves form the camera sensor to the memory and it encounters a series of processing steps, including quantization, shading connection, gamma amendment, filtering, white balancing and JPEG compression [6]. These handling ventures from clicking to storing pictures in the memory may

move on the basis of camera model. The four main methods that works on camera based digital image forgery detection are sensor noise, color filter array, chromatic aberration and camera response [5], [6]

3.4 Physical environment based digital image forgery detection

The peculiarities in the three-dimensional association between the camera, light and the physical articles can be demonstrated through picture forgery strategies dependent on physical condition. On account of the formation of a forgery with two film stars, the talk is that they are impractically strolling down a shoreline amid dusk [12]. Using the methods of splicing it is conceivable, yet the formation of the precise match in the lighting impacts is regularly troublesome with that of original photo [6], [7]. Here, the distinction in background lighting can be used as the altering proof. The functioning of the algorithm is on the premise of distinction in the lighting condition. 2D light detection, 3D light detection and light environment are the three main categories for this method [8].

3.5 Geometry based digital image forgery detection

This method measures the world items and the relative position of the camera. Principle point and metric measurement are two primary methods in geometry-based technique. Principle point is the projection of camera, focus to the image plane. The principal point for a picture is situated close to the focal point of the image [9]. When the picture object is changed, there is a relative change of principal point. This distinction in the assessed principle point of the picture can be utilized as the proof of altering. Getting metric measurement from a solitary picture is extremely valuable in forensic settings where true estimations are required [10], [11].

4 CONCLUSION

The need of digital image forgery detection is becoming more vital in this cutting-edge period. The altered images in military and court rooms can play an indispensable job in judgment or for important decisions. Through social media, journals and papers forged pictures can create detrimental actions or even devastate the life of an individual. The modern minimal effort software and tools empower the creation and control of digital pictures which leaves no distinguishable touches which follows with the goal of giving genuineness to the pictures that can be addressed as legitimate proof. There are several altering strategies, some of them discussed in this paper which address different parts of digital image forgery detection. Since passive techniques don't require any previous information, they are increasingly advantageous. Despite the fact that a significant number of these strategies are proficient to identify advanced picture altering, the need of present-day modern methods to detect digital image forgery is becoming more crucial.

References

1. Gill, N. K., Garg, R., & Doegar, E. A. (2017, July). A review paper on digital image forgery detection techniques. In 2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT) (pp. 1-7). IEEE.
2. Bharti, C. N., & Tandel, P. (2016, March). A survey of image forgery detection techniques. In 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET) (pp. 877-881). IEEE.
3. Huynh, T. K., Huynh, K. V., Le-Tien, T., & Nguyen, S. C. (2015, January). A survey on image forgery detection techniques. In The 2015 IEEE RIVF International Conference on Computing & Communication Technologies-Research, Innovation, and Vision for Future (RIVF) (pp. 71-76). IEEE.
4. Kashyap, A., Parmar, R. S., Agrawal, M., & Gupta, H. (2017). An evaluation of digital image forgery detection approaches. arXivpreprint arXiv:1703.09968.
5. Nampoothiri, V. P., & Sugitha, N. (2016, March). Digital image forgeryA threaten to digital forensics. In 2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT) (pp. 1-6). IEEE.
6. Walia, S., & Kumar, K. (2019). Digital image forgery detection: a systematic scrutiny. Australian Journal of Forensic Sciences, 51(5), 488-526.

7. Birajdar, G. K., & Mankar, V. H. (2013). Digital image forgery detection using passive techniques: A survey. Digital investigation, 10(3), 226-245.
8. Tembe, A. U., & Thombre, S. S. (2017, February). Survey of copy-paste forgery detection in digital image forensic. In 2017 International Conference on Innovative Mechanisms for Industry Applications (ICIMIA) (pp. 248-252). IEEE.
9. Johnson, M. K., & Farid, H. (2007, June). Exposing digital forgeries through specular highlights on the eye. In International Workshop on Information Hiding (pp. 311-325). Springer, Berlin, Heidelberg.
10. Ng, T. T., & Chang, S. F. (2004, October). A model for image splicing. In 2004 International Conference on Image Processing, 2004. ICIP'04. (Vol. 2, pp. 1169-1172). IEEE.
11. Nampoothiri, V. Parameswaran and N. Sugitha. Digital image forgery a threat to digital forensics. 2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT) (2016): 1-6.
12. Thakur, Tulsi, Kavita Singh, and Arun Yadav. "Blind Approach for Digital Image Forgery Detection." International Journal of Computer Applications 975 (2018): 8887.