IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 5, May 2022
Impact Factor: 6.252

Explainable Passive Image Forgery Detection

Akash Singh, Piyush Yogi, Prof. Vrushali Paithankar
Department of Computer Engineering
Smt Kashibai Navale College of Engineering, Vadgaon (Budruk), Pune, Maharashtra, India

Abstract: *The technical evolution of the world is conquering; the trust on the digital imaging technology is grinding down. In daily life, peoples come across the tampered or forged images from the tabloid magazines to the business industry. Furthermore in media outlets, scientific journals, political campaigns, courtrooms, and photo hoaxes that land in our email boxes, forged images are appearing more frequently in a unique way unable to identify the fake image with the needed sophistication. The nominal advancement from the film photography to digital photography is feasible boon but it is not trustworthy. The image tampering in the perspective of digital works can be considered as a creative work but there are some cases where the tampered images are being maliciously abused. Such critical condition arises where images seems to be the proof for the medical reports, crime scenes etc. where the forged image results in patients death and escape of the criminal respectively. The forging of the original image leads to illicit distribution, which raises the data famine problem. In research filed, the data owners are cautious about publishing their images without ownership and copyright which reduced the data availability for the researchers. Likewise, many problems arose in different fields because of the image forging.*

Keywords: Digital Forgery, Image Forgery, CNN

I. INTRODUCTION

In early years, film photography and the darkroom where found to be the answer for the visual representation Guillon,[7] but now the thing is contradictory. Digital images took its place in existence of the film photography with pluses Van Dijck.[13] Moreover, unlike conventional photography, the image capture by the digital cameras is easy, besides the storage and transfer is also feasible. In the cur- rent information era, the benefits of the digital images are exploited in different filed such as military, news, media, medical diagnosis, forensics, tabloid magazines, scientific journals, fashion industries, court halls and so on Watson and Null.[14] One of the central filed which fetched a notable gain is electronic commerce (Amazon, Snap deal etc.). Because of the advancement in IT and internet sector, the growth rate in E-Commerce has considerably increased in the recent years. In electronic commerce, the products are showcased with the images for the users and the users retail the online purchase only based on the image certainty, as per the world internet statistics, a growth rate of 160% has been reported in electronic commerce sec- tor from 2000–2005. Currently, 50 million internet users have made an online retail purchase. For every year, the cohort is expected to grow 100 million users. With the wide spread use of the internet, and availability of the different types of camera which are affordable at low prices, digital images is considered a major source of information in today's digital world Brinkmann.[4]

II. PROBLEMS TO DETECT IMAGE FORGERY

The major problems contained within for the detection of the image forgery are,

Data Provenance: Data source is the initial problem in the forgery detection. Vast number of images are available on the internet, in order to detect the forgery, the source of the original image is needed for the protection of rights and may be for supervisory prerequisite in applications like science, medicine, financial transactions government legal prosecutions and many more daily situations, wherever the information is valuable and trustworthy.

Benchmarking and Standard Data Set: The need for open data set for critical realisation of forging seems another problem in image forgery detection. The unavailability of the images in uncompressed for with different resolutions, sizes and image acquisition model with diverse contents are some of the needed image conditions for detecting the fake image from the original image which is critical to obtain.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 5, May 2022
Impact Factor: 6.252

Duplicate Regions: Duplication region appearance in the original image with same size, shape and colour appears to be another problem to detect the image forgery.

III. TYPES OF IMAGE FORGERY

The semantic information of an image is altered by addi- tion or extracting information from the image. In order to achieve the image forging, numerous ways are used by the forgers. In general, there exist different types of the image forgery. The categorization of the types of image forgery is a tedious task; this is because the forgery types are grouped based on the process involved creating the fake image. But in the current technical world, new inno- vations are made in the digital photography, which ascend new malicious forging techniques day by day. However, based on the existing types, a categorization is made in this research explaining different types of the image forgery Thajeel and Sulong.[12] Figure 1 depicts the different types of image forgery.

Examples of Image Forgery

Some of the examples of the different type of the forgery are presented in this section. Figure 2 depicts the exam- ple of image splicing. Figure 2(A) and 2(B) represents the original and Figure 2(C) represents the forged image. Here, the background of the original image containing cracks is retouched with a better background. Figure 3 signifies the example for copy-move image forgery. Figure 3(A) represents the original image which is forged as image shown in Figure 3(B) using copy-move image forgery.

IV. IMAGE FORGERY DETECTION

The need for the image forgery detection is increasing because of the threatening situation offered by the sophisticated image modification tools which diminish the cred- ibility and authenticity of the original image Farid.[5] This worse situation entails image forgery detection as an active area of research. Despite a hot topic in research commu- nity, only few works have been performed in image forgery detection but the need for more erudite detection algorithm is increasing. In fact, almost all of the image forgery detection techniques aim at detecting the composite operation (forgery type) used to manipulate the image.

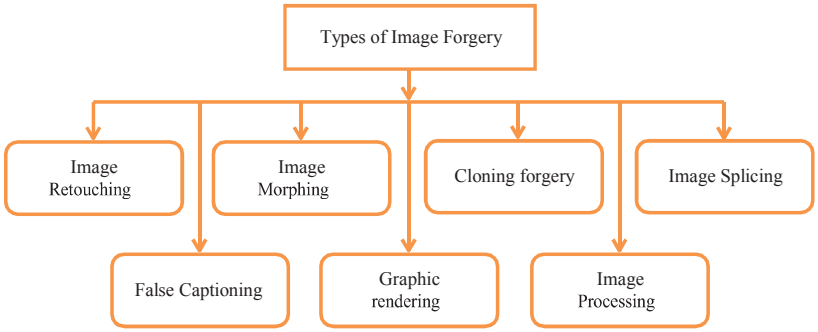

Fig. 1. Types of image forgery.

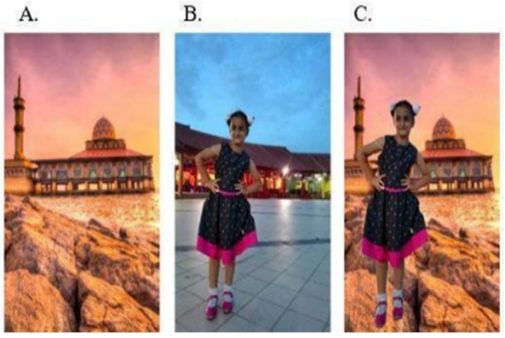

Fig. 2. Image Splicing

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 5, May 2022
Impact Factor: 6.252

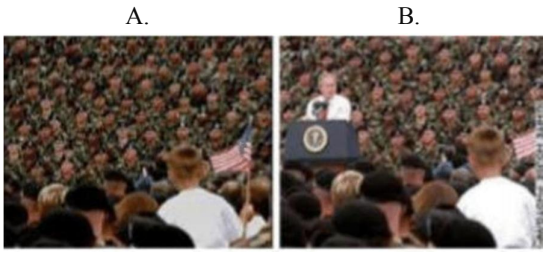

Fig. 3. Copy-move image forgery

At present different type of detection algorithms exist, but the general structure appears same with changes in concepts for detec- tion the fake images. The general structure of the image forgery detection is presented below. Figure 4 depicts the general structure of the image forgery detection. The image forgery detection is classified into two approaches centred on the prior knowledge requirement for the forgery detection. They are Active approaches based forgery detection and passive approaches based forgery detection.

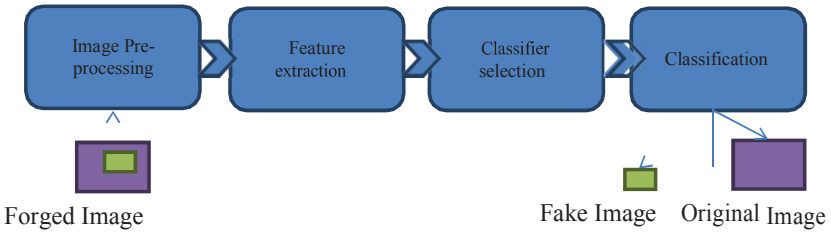

Fig. 4. General structure of image forgery detection

Active Approaches

Active forgery detection is the traditional method used for the detection of the image manipulation. Dynamic approaches verifies the authenticity of the image by means of hiding schemes. Watermarks or digital signatures are the data hidden in the image at the time of creation Al- Hammadi.[1] At the date of the recovery in the receiving end, the secret data or signatures are recovered and verified with the stored data for verification process. The original image may or may not be required at the received end during the check. The data recovery verification process in presence of original image is called non-oblivious data approaches and the data recovery verification process in absence of the original image is called oblivious data hiding method respectively.

Digital Watermarking

In digital marking based active approaches, a particular digest is inserted into the original image at the time of capturing. The authenticity of the image can be verified at any instance by extracting the digest. When the digest differ from the original one, the image is considered as a manipulated image. Judith et al.[9]

Digital Signature

In digital signature based active approaches, the unique properties of the captured image are extracted as signa- ture from the image at the capturing end. In authentication process, the properties of the pictures are regenerated and matched. While matching, if the signature is found varied, the image is considered as tampered image BarnaliSarma and Gypsy Nandi.[2]

Passive Approaches

Passive forgery detection criteria are exact contradictory of the active approaches. Passive approaches authenticate the tampering of the image without any prior knowledge of the original image or its features. In order to verify the genuineness of the image, the statistics and content of the available image are utilized in the passive approaches. The verification process is performed based on the infor- mation of the picture itself without using any additional information. Since the passive approaches authenticate the forged image based on the available knowledge, it is also called as blind approach. The brief introduction about the passive approaches based forgery detection techniques is available in Mahdian and Saic.[11] Figure 5 specifies the decisive steps involved in the forgery detection.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 5, May 2022
Impact Factor: 6.252

Pixel Based Techniques

Pixel based techniques identify the forgery in the original image by analysing the pixels constituting the image. The processing steps involved in the pixel based techniques are, primarily, the image pixels of the test images are evalu- ated and the image pixel collection having random inten- sity signifies the fact that the images are forged. Pixel inter correlation occur in forged images either directly or indirectly because of the tampering operation either with small semantic information change or with larger semantic information change. In initial works of pixel based tech- niques, instead of pixel, the block analysis is performed to detect the ambiguousness. In block based methods, the image subjected to forgery authentication is divided into blocks and individual blocks are matched with each other. The image block which differs from others resembles the localized area of tampering. Principal Component Analy- sis (PCA) Fridrich[6] is the most prominent techniques used for searching matching blocks in the image.

Format Based Techniques

Format based techniques detect the forgery in the images based on the changes in the image format. The steps involved in the format based techniques are, primarily, the images are divided into DCT blocks and quantized which results in coefficients. The quantization coefficients are determined from the quantization table. This is one of the compression techniques. This raises certain artifacts in the image which can be used for the forgery detection. The artifacts occurrence is because of the presence of horizon- tal and vertical edges between the blocks due to indepen- dent transformation and quantization of each block from other blocks. The quality of the image and its size is deter- mined by the quantization table, tends to differ between camera manufacturers which can exploited to perform a forensic analysis on the image to determine its source cam- era Liu et al.10

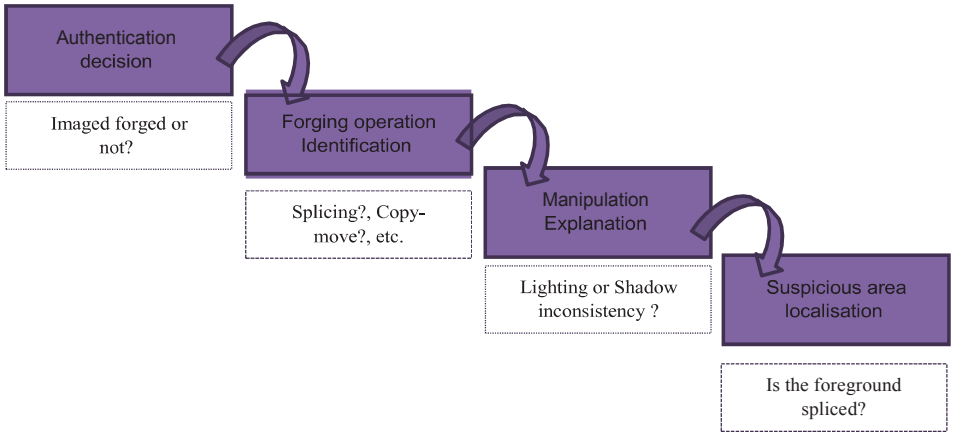

Fig. 5. Decisive steps in forgery detection

Camera Based Techniques

Camera based techniques detect anomalies in the image by exploiting the artifacts introduced by the camera lens, imaging sensor, sensor noise etc. Inconsistencies in these artifacts can be used as evidence of tampering Bayram et al.3 The processing steps involved in the camera based techniques are, primarily, the camera is used to capture the image. Some artifacts are present associated with the cap- tured image because of the aberration in the camera lens, imaging sensor, etc. These artifacts manifest the presence of image forgery because of varying characteristic of the camera.

Forgery Shadow Detection

Shadows are essential part of an image. The shadow based detection is the most convenient forgery detection proce- dure Zhang et al.15 This is because, when a forger tampers the image, the only concentration is centred on manipu- lating the objects present in the image which results in shadow inconsistencies of the image. By analysing the shadow properties of the image, the tampering operation performed for the manipulation can be recognised. The shadow in the image is formed by the unruffled action of the light source and the occluding object present at the time of capture.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 5, May 2022
Impact Factor: 6.252

Forgery Reflection Detection

Forgery reflection based detection is another crucial forgery detection methodology James and Farid. This type of detection method utilizes the inconsistencies of the image reflection for the forgery detection. Reflection occurs in an image, when the light from the source bounces off a surface and penetrate through the aperture of the plane mirror.

V. CONCLUSION

Authenticity and integrity of the digital images are well- thought-out to be important to overcome these issues because of the forging in fields such as forensic, medi- cal imaging, e-commerce, industrial photography, etc. The authenticity verification check of the image is popularly used where the images are considered to supporting evi- dences, historical records, insurance claims, etc. Because of the drastic increase in the software availability for the advanced image manipulation and processing, the original images are tampered without leaving any trace for forgery detection. This results in revising the old saying "A pic- ture is worth a thousand words" to "A picture unworthy a thousand true words." This study concluded the different types of image forgery and approaches to be available in the research community.

REFERENCES

[1]. M. Al-Hammadi, Copy Move Forgery Detection in Digital Images Based on Multiresolution Techniques, King Saud University, Riyadh (2014), Vol. 13, pp. 741–756.
[2]. BarnaliSarma and Gypsy Nandi, International Journal of Advanced Research in Computer Science and Software Engineering 4, 878 (2014).
[3]. S. Bayram, H. Sencar, and N. Memon, Improvements on source cam- era model identification based on CFA interpolation, Proceedings of IFIP International Conference on Digital Forensics (2006), Vol. 12, pp. 289–299.
[4]. R. Brinkmann, The Art and Science of Digital Compositing, Aca- demic Press, San Diego (1999), Vol. 12, pp. 776–789.
[5]. H. Farid, IEEE Signal Processing Magazine 26, 16 (2009).
[6]. J. Fridrich, B. Soukal, and A. Lukas, Detection of copy-move forgery in digital images, Proceeedings of Digital Forensic Research Work- shop (2003), Vol. 3, pp. 90–105.
[7]. J. P. Guillon, Journal of the British Contact Lens Association 5, 8486 (1982).
[8]. O. James and H. Farid, Exposing photo manipulation with inconsis- tent reflections, Proceedings of ACM Transaction on Graphics 31, 1 (2012).
[9]. A. Judith, T. Wiem, and D. Jean-Luc, Multimedia Tools and Appli- cations 51, 133 (2007).
[10]. M. Liu, N. Yu, and W. Li, Camera model identification for JPEG images via tensor analysis, Proceedings of International Conference on Intelligent Information Hiding and Multimedia Signal Processing (2010), Vol. 1, pp. 462–465.
[11]. B. Mahdian and S. Saic, IEEE Transactions on Information Foren- sics and Security 3, 529 (2008).
[12]. S. Thajeel and G. Sulong, Journal of Theoretical and Applied Infor- mation TechNology 70, 245 (2014).
[13]. J. Van Dijck, Visual Communication 7, 57 (2008).
[14]. A. B. Watson and C. H. Null, Digital images and human vision 23, 123 (1997).
[15]. W. Zhang, X. Cao, J. Zhang, J. Zhu, and P. Wang, Detecting photo- graphic composites using shadows, Proceedings of the IEEE Inter- national Conference on Multimedia and Expo (ICME '09) (2009), pp. 1042–1045.