A comparative study on image forgery-facial retouching

Kinjal Ravi Sheth, Vishal Suryakanthbhai Vora
Department of Electronics and Communications Engineering, Faculty of Engineering and Technology, Atmiya University, Rajkot, India

ABSTRACT

Forgery with the digital images is being very easy now days due to the very advanced and open source image editing tools, software and devises which supports a high quality of resolutions. Tempering with digital documents for changing identity or sometimes for fun is increasing day by day as the era is of digital world. Detecting clues of tampering and verifying the authenticity of images is an important issues now-a-days and growing research field. The existing research in the area of digital image forgery identification is discussed here. Different types of image forgery attacks along with its detection and classification are discussed too. A general review of facial image authentication is studied and discussed here along with the current methods and techniques for the detection and classification. A comparative analysis is presented here for the researchers as a mind mapping to work in the same field.

Keywords: Active forgery Detection Image forgery Passive forgery Retouching

1. INTRODUCTION

As in today’s world, everything is in terms of 1 or 0, most of the public is spending their time on digital platform. Started from the profile photo on digital media to upload the photo on matrimonial site everything becomes so easy. Started with uploading a single document to passport size photo is now possible because of user friendly smart phones available on a fair rates and with free apps [1]. The authenticity of photographs is critical because they are frequently used as supporting documents or as records in a variety of applications, including criminal studies, news photography, forensic science, law-enforcement, claim of insurance, medical imaging, and matrimonial sites. As per today’s scenario, image forensic is a growing field where the major objective is to detect thetempering or forgery in images. Forgery can be done with or without the prior knowledge of original image. Active forgery and passive forgery are the main classification of forgery attacks. The detection of active forgery is quite simpler as one could have clue about the original image, such as watermarks or digital signatures [2]. On the contrary, a passive forgery detection is a techniques which requires no prior information of the image for verification; hence, it is very difficult to identify or authenticate the original image [3], [4]. Passive image forgery is further classified as copy move, rescaling, resizing and retouching. The forgery can be done on images including natural scenes, beauty, face images or any living or noon living things. The analysis of forgery attacks taken place on facial images is carried out in this paper, as malfunctioning with facial photos done very frequently intentionally or for fun on social media or for authentic proof. The detection of forgery is manipulated with the advanced machine learning and deep learning algorithms [5].

The paper is organised as introduction of the image forgery followed by the section 2 which includes why and when the development of forgery detection methods has been done. In section 3, we discuss about...
the classification of forgery attacks and methods. As mentioned, the demanding use of social media increasing the spoofing of facial images. That is illegal no matter whether it is done intentionally or unintentionally. Section 4 includes the basics and fundamental of facial forgery. Sections 5 and 6 give the survey and comparative analysis on existing methods adopted for detection and classification of facial forgery. In section 7, we conclude the paper with some ideas of future works.

2. DEVELOPMENT OF IMAGE FORGERY DETECTION METHOD

Looking to the current scenario with reference to digital image, forgery means any kind of tempering or doctoring which can change the intensity of image for any illegal purpose or use [6]. According to the Wall Street Journal records, about 10-15% of the photos published in the U.S. in 1989 were fabricated [7]. Manipulation of digital image became more popular in the 20th century to assist political publicity, and it is currently utilised for matrimonial sites, multimedia or social media to some extent for pleasure. Previously, images were modified through retouching with negatives, ink, and paint [8]. Due to unavailability of the insufficient technology and powerful capturing devices tampering was difficult. Hippolyte Bayard, a photographer from French, was the first one who manipulated the original image in eighteen forty with the titled: “Self picture as a drowned man”. Figure 1 shows the image in which he had shown that he had tried to commit suicide [8]. Figure 2(a) shows the photo of American commanding general seating on horse during American civil war. More than a decade ago, it was time of civil war of America where a photograph of commanding general was viral which indicates that general was sitting on the horse in the visible side of the crowds near the city Virginia [5]. Later on it has been found that it was not an original image but it’s a composition of three different images which has been created from the negatives. Referring Figure 2(b), in this case the Iran has been caught by tempering the image based on the missile test. This image was displayed on the genuine site if the Iran’s government which states that four one by one simultaneously successfully launch of missiles [8]. In third case, as shown in Figure 2(c), in two thousand seventeen a forged image of Mr. Putin—the President of Russia has been viral over the internet regarding meeting with Mr. Trump—the USA President.

Figure 1. First image forgery reported

Figure 2. Images illustrating image forgery attacks (a) a photo of American commanding general, during American civil war, (b) Iranian montage of missiles, and (c) fake image of Putin met with Donald Trump during the G20 summit 2017 (right), original image (left)
3. CLASSIFICATION OF FORGERY DETECTION

Tampering of images becomes successful with the knowledge and understanding of properties of the digital image. Tempering with the images are not always done for propagating the wrong information to the society or to target someone but sometimes images are tampered for adding security to authenticate the documents with digital signatures or sometimes are used only to manipulate photos for enjoyment. Image tempering identification methods are mostly categorised in two ways: active and passive [8]. In general, active tempering detection methods require some information before to process. Digital watermarking and signature are the methods is being worked as an active method in which the prior knowledge of algorithms and the image to be inserted is required [9]–[16]. With the help of these method to detect the integrity of the original and doctored image. Considering domain specific these methods can be divided on fragile, semi-fragile by calculating the robustness and perceptual transparency of the image. In real time cases it is very rare to generate the image which can later use in investigation process contains the watermark to check the authenticity and integrity therefore it can be said of active techniques are rarely used in the investigation and detection process.

Whereas a passive forgery detection technique identify manipulations by extracting either all or some of the features of the image without need of prior information of the image or verification; such as watermarks or digital signatures. This technique is being divided in based on dependant and independent forgery. In dependent forgery, the same image is being tempered by copying some data of the image and pasted on the other area of the image. More than one image can be clubbed together will be considered as dependant forgery [17], [18]. While in case of independent method, it is being classified as retouching, scaling [19], rotation, means you cannot be altering the content of the image but different filters are being applied to enhance or degrade the quality of images. Figures 3 and 4 shows the categorical structure of active and passive forgery techniques. The most prevalent forgery attempts are copy-move, splicing and retouching. Figure 5 shows the work done till now on different forgery attacks by submitting the query based on words on google scholars. Copy-move attack is one of the easiest forgery where some portion of image is copied and pasted to some other region of the same image. A comparative analysis based on hand crafted and machine crafted features for copy-move forgery detection is presented in [5]. Various image copy-move forgery detection algorithms based on convolutional neural network (CNN) and deep learning are evaluated and concluded that CNN based image copy-move forgery detection (IC-MFD) algorithms are more effective, less time consuming and uses up less resources too [20].

![Figure 3. Classification of active image forgery](image1)

![Figure 4. Classification of passive image forgery](image2)
A broad literature review is presented in [21] on image forgery detection with deep learning approach which have accomplished high performance accuracies in context with image or facial image. Research by Ahmed et al. [22] focuses on SFTA, Haralick, and LBP as feature extraction methods followed by features fed to KNN classifier to detect and classify the copy-move attack. The rust shows that k-nearest neighbors (KNN) classifier gives result accuracy of 81.81%, 86.36% and 95.45% for segmentation based fractal texture analysis (SFTA), local binary patterns (LBP) and haralicks respectively. When scaling, rotation and compression operation are done on image, it becomes to difficult to detect tempering. A framework is presented in [23] to perform an optimization of digital forgery techniques in cost effective way.

5 level of framework is proposed which includes: i) image block partition to detect locally tempered region of image, ii) extracting primary attributes on the basis of colour mosaic, iii) binary classification, iv) mitigate complex attack, and v) performance analysis.

4. FUNDAMENTALS OF IMAGE RETOUCHING

Image retouching is a kind of blind forgery technique that is frequently employed for commercial and aesthetic purposes. Retouching means “to polish the image”. In such forgery, more frequently, modify the facial image or photo using any image editing tools which if easily available in order to achieve some specific result. However, this type of forgery is seen in entertainment media, magazine covers, social media profile, matrimonial sites, where retouching is used only for making the image more attractive or beautiful. Hence, facial beautification plays very essential role in such type of attacks and so, for numerous decades, face recognition and retouching detection has been a very active research subject. Mainly 3 types of facial beautification can be achieved in practice: i) plastic surgery, ii) facial cosmetic, and iii) retouching. All these 3 types of beautifications more or less corrects or changes the facial features to make the appearance more attractive, appealing or funny sometimes. Advertisers, fashion publications, and fitness magazines have always worked to create a fantasy for their consumers in order to grow their business. The photos published by those, however, are often the result of image retouching in digital sense. But this is considered to be equivalent to an offence or ethically wrong if the forged image is used as a matrimonial profile or as a social media profile to mislead someone [24], [25]. Basic colour or contrast correction, glamour retouching, skin tone retouching, photo restoration, photo cartooning, and other treatments are all part of facial retouching [8]. Fine image enhancement, colour or contrast changes and illumination or brightness changes the original facial image into the forged image. In addition, further modifications can be achieved such as resizing of chin, ear, nose, enlarging of eyes or mouth or varying the texture or style or colour of hair. Finally, if the real image is unknown, detection is difficult, therefore blind detection is a difficult task. One best example for spoofing is explained here with Figure 6 [26] where by applying suitable filtering the wrinkles are disappeared. Literally, such type of manipulation is ethically wrong. Because this creates negative impression on viewer’s mind and may push the viewer in mental disorder or depression sometimes. So to overcome such situation, Photoshop Laws have been issued [27] stating that faces and bodies images or photos that have been altered must be labelled because they can generate a mistaken perspective of reality.
5. EXISTING ALGORITHMS

The purpose of retouching is to enhance or minimise the image's attributes. Advertisers, fashion publications, and fitness magazines have always worked to create a fantasy for their consumers in order to grow their business. Impractical attractive and immaculate models with exquisite physiques were frequently featured on magazine covers and commercials [28]. These photos are mostly the result of digital retouching known as appearance-based image alteration. The aim of this study is to look into all of the existing dependent passive forgery approaches for detecting facial doctoring attacks, as well as recent developments in this challenging sector. We hope that this review will serve as a beacon and will help the researchers from the image forgery detection area to identify new research problems. This section summarizes the existing works based on facial retouching, detection and classification of original image and retouched image.

The retouching operations alter facial characteristics such as skin texture and tone, shape of eyes, eyebrows, nose, lips, chin or overall face, elevation of smile and forehead, eye colour and hair texture. Performance are most commonly rated with standardized parameters for measuring biometric performance which is explained in detailed in [29], like equal-error-rate (EER) or false error rate (FER) and for detection schemes, the correct classification rate (CCR). Retouched photos published by magazine or on advertise are globally broadcast and the idealised and unrealistic representation of physical attractiveness has been developed in public mindset. Certain countries have mandated that advertisement photos must indicate whether the photo has been digitally retouched or not, as per the “photo-shop law” [24], [25], [30]. This paper summarises the technical considerations and back-and-forth of the studied approaches, as well as open difficulties and challenges in the field of facial retouching and recognition. Three types of face alterations plastic surgery, make up and facial retouching are discussed and the published literatures are compared [31]. Some researchers have demonstrated that the presence of makeup on the face reduces the performance of facial recognition systems. A makeup detector is suggested in [32] to further lessen the influence of cosmetics on face identification where youtube makeup database (YMD), makeup in the wild (MIW) and facial cosmetic database (FCD), publicly available datasets, are used. The suggested method extracts the feature vector that collects the texture and shape information of the input face and analysed the degree of makeup. The first publicly available plastic surgery database provided by [33], intended for face recognition research. Nose and chin surgery, cheek implant, Skin peeling and eye brow lifting are only a few of the procedures covered in this database (face lift) [33]. Six recognition algorithms based on look, feature, and texture were chosen and mentioned to evaluate the effect of plastic surgery on face recognition, and concluded that these algorithms are not able to successfully offset the variation caused by plastic surgery treatments. The impact of digital beautifying on face recognition systems was studied by Ferrara et al. [34]. In compared to geometrical distortions, the author reported notable performance degradation for various face recognition systems if heavy facial retouching is applied on images. Ferrara et al. [34] had worked to face recognition for the images used for specifically authentication i.e. as electronic identity documents which are altered purposely or unintentionally. The AR face dataset was used, which contains 4,000 high-quality facial pictures shot over two weeks in two sessions in varied circumstances with neutral emotions and decent illumination. To obtain retouching, LiftMagic and antiaging make over tool [35] is used that creates realistic beauty enhancement in image [34]. Barrel distortion, vertical contraction and extension was performed over the face images, which actually represents the image alteration by a poor quality camera. The experimental results presented by the author shows that the barrel distortion does not have a substantial impact on the accuracy of recognition. According to Bourlai [36], extended the work with new dataset including morphed images. The performances are compared with 526 genuine attacks, 19944 impostor attempts and 160 morph attacks and the performance computed based on EER, false acceptance rate (FAR) and morphed acceptance rate (MAR). An approach is proposed and discussed to detect facial wrinkles/imperfection by gabor filter response using gaussian mixer model and EM algorithm by Batool et al. [26]. The SCUT-FBP database was created and presented by Xie et al. [37]. The dataset contains 500 better resolutions, front end face images of Asiatic female with neutral pose, plane background, no add-ons and minimal occlusion. An evaluation for the SCUT-FBP database based on traditional machine learning and deep learning approaches is_A comparative study on image forgery-facial retouching (Kinjal Ravi Sheth)
proposed by Xie et al. [37]. The Pearson coefficient for performance measurement around 0.8187 was achieved with CNN approach. Bharati et al. [38], [39] proposed facial image retouching detection based on machine learning and deep learning with different classifier as well created a database which is one of the publicly available datasets. Different deep learning methods with various classifiers are suggested to differentiate between real and retouched or fake facial images. Moreover, the results are compared with human performance. Jain et al. [40] presented a CNN architecture for detecting digital manipulations on real ND-IIITD images and GANs based alterations. The results are experimented on two different datasets: ND-IIITD database [41] and images generated using StarGANs.

Research by Hulzebosch et al. [42] established a framework for analysis the detection methods in real-world settings, which included cross model, cross data, and post processing steps. The suggested framework was utilised to evaluate state-of-the-art detection approaches. Dang et al. [43] suggested a mechanism to process for the classification job rather than just applying multi-tasking learning to detect modified images and anticipate the altered mask (regions). The proposed algorithm highlights the informative areas to further improve the digital classification (real face vs doctored face). AI tools are coming to us in variety of ways, some of which are beneficial but some could be misused against us. One of the best examples of that is deepfake. Deepfake is used to totally alter any video or image content into something unoriginal. A survey is presented by Aminu et al. [23] to understand deepfake and how to prevent malignant deepfake. Digital forgery forensic algorithms and tools are developed to detect the manipulation over original images. The detail classification and evaluation for some of the software forensic tool i.e., foto forensic, IZitru, JPEGsnoop, forensically and ghifo has been carried out in [44] and concluded that some tools are not reflecting the basic concepts, like feature extraction and selection, used for detection of forged images.

6. A COMPARATIVE ANALYSIS OF DIFFERENT EXISTING METHODS

This section is managed between the survey papers and existing modern algorithms used for recognition and detection of facial forgery and the performance analysis. The list of survey papers available for the basic study of image forgery, its types and techniques are included in Table 1. Few state-of-the-art techniques used for detect different types of facial image forgery are shown in Table 2. In this table, the analysis of facial retouching procedures is presented in tabular format based on numerous factors, including dataset, software tool utilised, and performance achievement.

<table>
<thead>
<tr>
<th>Sr. No</th>
<th>Title Description</th>
<th>Contribution</th>
<th>Observation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>A survey of passive image forgery detection [45]</td>
<td>Categorised forgery detection in to low-level, middle level and high level.</td>
<td>Targeting the issues related to public image database and performance evaluation, usability, detection strategy to point out for forgery attack and detection. Existing approaches are not automated and the results must be interpreted by humans. The methods are ineffective when small regions are copied and moved. Existing biometric anti spoofing is divided into three categories: i) sensor-level: are highly accurate for picture, video, and mask attacks, but are costly and time consuming, ii) feature-level: are ineffective in single-face image scenarios and have low video attack accuracy, iii) score-level: Existing techniques suffer from limitations like less detection accuracy and high computation complexity. With regular background, rotation scaling, compression and blurring it gives lots of false matches. It is suggested to extend the research to detect forgeries in videos.</td>
</tr>
<tr>
<td>2</td>
<td>Digital image forgery detections using passive techniques: a survey [46]</td>
<td>Forgery detection algorithms are reviewed with a focus on passive forgery and detection.</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Biometric antispoofer: a survey in face recognition [47]</td>
<td>An overview of the research that has been done in the burgeoning field of anti-spoofering on the face modality.</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Deepfake: a survey on facial forgery technique using generative adversarial network [48]</td>
<td>Presented review of working of deepfake technique and the ways to identify if the video is generated by deepfake. Comprehensive analysis to detect Deepfake video using different methods like recurrent neural network and MesoNet.</td>
<td>Deepfake technique with the generative adversarial network can generate an output, which looks realistic to human eyes</td>
</tr>
<tr>
<td>6</td>
<td>Survey on blind image forgery detection [49]</td>
<td>Reviewed passive forgery detection techniques and categorized into mainly 3 attacks: copy-move, splicing, retouching</td>
<td>DCT-based techniques are ineffective when considering highly textured and small altered regions.</td>
</tr>
</tbody>
</table>
Table 2. Relevant work done on the detection and classification of facial retouching

<table>
<thead>
<tr>
<th>Sr. No</th>
<th>Title</th>
<th>Database</th>
<th>Beautification detection accuracy</th>
<th>Tools used for retouching</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>On the impact of alteration on face photo recognition and accuracy [34]</td>
<td>AR faces</td>
<td>-2%, -5%, -17% EER for low/medium/high intensity</td>
<td>LifiMagic</td>
</tr>
<tr>
<td>2</td>
<td>Detecting facial retouching using supervised deep learning [38]</td>
<td>ND-IIITD dataset</td>
<td>87.1% CCR and ND-IIITD dataset</td>
<td>PortraitPro studio Max</td>
</tr>
<tr>
<td>3</td>
<td>Demography-based facial retouching detection using subclass supervised sparse autoencoder [39]</td>
<td>Multi demographical retouched faces</td>
<td>94.3% correct classification rate (CCR)</td>
<td>BeautyPlus, potraitpro studio Max</td>
</tr>
<tr>
<td>4</td>
<td>On the detection of digital facial manipulation [43]</td>
<td>ND-IIITD dataset and StarGAN</td>
<td>99.70% (Thresholding) and 99.42% (SVM)</td>
<td>PortraitPro Max</td>
</tr>
<tr>
<td>5</td>
<td>On the generality of facial forgery detection [50]</td>
<td>Deepfakes</td>
<td>~20%</td>
<td>GANs</td>
</tr>
<tr>
<td>6</td>
<td>PRNU-based detection of facial retouching [51]</td>
<td>FRGCv2 face database</td>
<td>~13.7% detection-equal error rate (D-EER)</td>
<td>Airbrush, fotorush instabeauty, PolarR</td>
</tr>
<tr>
<td>7</td>
<td>Detecting CNN-generated facial images in real-world scenario [42]</td>
<td></td>
<td>Average fake images detection accuracy 86.7% (highest) and 37% (lowest)</td>
<td>StarGAN, ProGAN, GLOW, StyleGAN</td>
</tr>
</tbody>
</table>

7. CONCLUSION AND FUTURE WORK

With the help of internet any one can easily destroy the life by spreading any kind of forged image. The editing tools are easily and freely available in the market that cannot be easily traced after the alteration of images. Areas like Law enforcement offices, private sectors, government departments, education institutes, everywhere such types of detection methods play a very significant role in decision making process. There are several issues need to pay attention when we proposed new algorithm for forgery detection and classification based on this literature review; i) several algorithms have been discussed here with performance rating. The performance comparison is obvious when more and more algorithms are developed for spoofing attacks. This can be possible if and only if we have one unique public database is available which includes many kinds of authentic images with tempered images, ii) many more detection algorithm detects specific kind of spoofing done over facial images like changes in hair color, eyes color. Usability cannot be disregarded if we want facial forgery detection algorithms to be useful in real-world applications, and iii) tempering on the facial images can be done globally or on some part of the images. Hence, not all the methods detect and identify that the tempering done globally or locally. Therefore, it is a sensible decision to check for discrepancies of specific statistical properties of a picture for tampering detection.

REFERENCES


A comparative study on image forgery-facial retouching (Kinjal Ravi Sheth)

BIOGRAPHIES OF AUTHORS

**Kinjal Ravi Sheth** is an Assistant Professor at L D Collage of Engineering, Ahmedabad, Gujarat, India since 2011. She is also a Ph.D research scholar of Atmiya University at Department of Electronics and Communication, Rajkot, Gujarat, India. She has completed her master of engineering from Dharmasinh Desai University, Nadiad in 2008. Her area of interest is image processing, machine learning, and satellite communication. She can be contacted at email: kinjal.ddit@gmail.com.

**Dr. Vishal Suryakanthbhai Vora** is in charge head of Department of Electronics and Communications Engineering and Physics both, at the same time he is also the coordinator of exam section for Atmiya University. He has 14 years of experience in academics and administration. His passion lies in transform the life of students by encouraging them and give them knowledge about technical skills with value education. He can be contacted at email: vsvora@aits.edu.in.