Multimedia Tools and Applications (2023) 82:14153–14169
https://doi.org/10.1007/s11042-022-13699-x

An image forensic technique based on JPEG ghosts

Divakar Singh[1] · Priyanka Singh[2] · Riyanka Jena[2] · Rajat Subhra Chakraborty[3]

Received: 2 May 2022 / Revised: 11 August 2022 / Accepted: 15 August 2022 /
Published online: 30 September 2022

Abstract

The unprecedented growth in the easy availability of photo-editing tools has endangered the power of digital images. An image was supposed to be worth more than a thousand words, but now this can be said only if it can be authenticated or the integrity of the image can be proved to be intact. In this paper, we propose a digital image forensic technique for JPEG images. It can detect any forgery in the image if the forged portion called a ghost image is having a compression quality different from that of the cover image. It is based on resaving the JPEG image at different JPEG qualities, and the detection of the forged portion is maximum when it is saved at the same JPEG quality as the cover image. Also, we can precisely predict the JPEG quality of the cover image by analyzing the similarity using Structural Similarity Index Measure (SSIM) or the energy of the images. The first maxima in SSIM or the first minima in energy correspond to the cover image JPEG quality. We created a dataset for varying JPEG compression qualities of the ghost and the cover images and validated the scalability of the experimental results. We also, experimented with varied attack scenarios, e.g. high-quality ghost image embedded in low quality of cover image, low-quality ghost image embedded in high-quality of cover image, and ghost image and cover image both at the same quality. The proposed method is able to localize the tampered portions accurately even for forgeries as small as 10×10 sized pixel blocks. Our technique is also robust against other attack scenarios like copy-move forgery, inserting text into image, rescaling (zoom-out/zoom-in) ghost image and then pasting on cover image.

✉ Riyanka Jena
201921012@daiict.ac.in

Divakar Singh
2019pcs0020@iitjammu.ac.in

Priyanka Singh
priyanka_singh@daiict.ac.in

Rajat Subhra Chakraborty
rschakraborty@cse.iitkgp.ac.in

[1] Indian Institute of Technology Jammu, 181221, India

[2] Dhirubhai Ambani Institute of Information and Communication Technology, Gandhinagar, 382004, Gujarat, India

[3] Indian Institute of Technology Kharagpur, 721302, West Bengal, India

Keywords Forgery · JPEG compression · Quality · SSIM

1 Introduction

We are in an era where technology is advancing at a boost-up rate, and with every such boom comes a curse. In this case, the advancement of technology provides anyone the ease to edit/manipulate the image leading to a resultant forged image that is hard to trace, causing a loss of integrity of the image. Nowadays, many fake images are created which can be harmful in many possible ways. In today's digital era, the authenticity of digital data is a prime concern. Image editing software like Adobe Photoshop, Fotor, etc. are readily available which enables the creation of more and more fake images. Some of the areas where image forgery causes irreparable damage are the banking domain (account fraud, cheque frauds), and identity theft. Most of the applications we preferably used JPEG images as they help to save bandwidth and can be compressed as per the need. Hence, in this work, we propose techniques to safeguard forgery in JPEG images against various attack scenarios and localize the forged areas accurately even for very small sized tampered areas. They may be very critical to decision-making of crucial applications like land revenue documents forgery, certificates with seals and signatures, etc.

Although many schemes have already been proposed in the literature that addresses various image forgeries still we keep viewing instances of forgeries, e.g. a duplicate move fabrication where a gathering of warriors was copied to cover an image of George Bush [21]. A doctored image of a Malaysian politician Jeffrey Wong Su showing him as a knight by the Queen of England in July 2010 [7]. Another recent news was of a photo shared on Facebook in 2020 to falsely claim that the people in this photo were coronavirus victims in China, but in reality it was a photograph of an art project in Germany in 2014 [11] and many more [8] With high-end editing technologies, it has become really challenging to keep pace with the kind of possible forgeries and their revelation.

Digital image forgery means manipulating a digital image to conceal some meaningful or useful information that would otherwise be conveyed by the image. There are several cases when it is difficult to identify the manipulated/adulterated region of the image. The detection of a forged image is driven by the need for authenticity. Recent advances in digital forensics have given rise to many techniques for detecting photographic tampering. These include techniques for detecting cloning [10, 24], splicing [23], resampling artifacts [2, 25], color filter array aberrations [25], sensor noise pattern [19], chromatic aberrations [15], and lighting inconsistencies [16]. Advanced methods like detecting image manipulation based on edge detection and faster R-CNN [31], image splicing localization using a Multi-task Fully Convolutional Network (MFCN) [28] and automatic JPEG ghost detection [3] were recently proposed.

Methods proposed to detect forgery can be broadly categorized as the active methods and the passive methods. In the active approach, certain information is added into an image during the creation of a digital watermark [14]. In the passive method, there is no requirement of active data for authentication of the picture.

In this paper, we propose a passive method to detect image forgery based on the difference in the JPEG qualities of the forged portion and rest of the image. The original image is referred to as the cover image and the forged portion is called as a ghost image. The localization of the forged portions is done based on resaving the forged composite image at different image qualities and then finding the range of JPEG qualities where the detection of forgery is maximum. We have experimented with varied combinations of ghost and cover image qualities and also contributed a dataset for scalable testing. The experiments are carried out for varied attack scenarios and analysis of forgery localization done using SSIM and energy of the difference image. Following are the key contributions:

- Dataset: We have constructed a sufficiently large dataset for the forgery detection based on JPEG qualities. A composite image that is a combination of ghost and cover image quality is saved at different JPEG qualities in the range of 40 to 100. We tried to cover the maximum combinations of JPEG qualities for the ghost and the cover image.
- Better localization of forged areas: For detection of forged portion, we are using a YCbCr color space. In YCbCr color space, the luminance and chrominance components are separated and so it helps the Human Visual System (HVS) to better localize the forged portions.
- Prediction of image quality: We analyzed the forgery detection results using SSIM and energy graphs and found that the cover image quality can be predicted from these plots. The cover image quality corresponds to first maxima in SSIM plot and first minima in energy plot.
- Varied attack scenarios: We experimented the proposed method with a variety of scenarios to check the robustness of the scheme. To be specific, combinations of high quality ghost-low quality cover, low quality ghost-high quality cover, equal JPEG quality for ghost and cover for copy-move forgeries. Also, we considered forgery like inserting text into images, rescaling (Zoom-out/Zoom-in) of images and ability to detect very small forged ghost portions.

The rest of the paper is organized as follows. Section 2 discusses the related work. The proposed method is discussed in Section 3. Various experiment scenarios are discussed in Section 4 along with the details of the dataset. Conclusion and future directions are outlined in Section 5.

2 Related work

To detect image forgery, several schemes have been proposed in the literature. Here, we briefly discuss some of these and their limitations.

In [24], the authors used a technique related to duplicated image regions where they describe an efficient approach that automatically detects copied areas in a digital image. This technique works by applying a principal component analysis to small fixed-size image blocks to yield reduced representation. The accuracy is, in general, excellent, except for small block sizes and low JPEG qualities. The detection rates are nearly perfect, except for small block sizes and low signal-to-noise ratio (SNR).

The authors of [2] proposed a method based on the assumption that in creation of doctored images, there is always some processing/operations that is done on the images which give rise to measurable distortions in the image properties. They utilized these distortions to classify the images into original verses processed or doctored images. The method was limited to detect forgeries in image regions of dimension at least 100 × 100 pixels, not below that which was crucial to many sensitive applications.

In [19], the authors presented a technique for image forgery detection by checking any distortion in the underlying photo response non-uniformity (PRNU) pattern of the image. PRNU is a unique pattern that can be associated to a specific camera. Any images that are clicked from that camera will have this underlying pattern. Even if two cameras are of make same and model, they will have different PRNU patterns. They proposed their scheme for scenarios when the camera that clicked the photo is available or other images clicked from the same camera are available. They also investigated their scheme for various image processing operations such as lossy compression or filtering and how it influences the ability to verify image integrity.

The approach in [20] proposed a scheme exploiting the symmetry of the blocking artifacts in JPEG images to detect tamper for a cropped and re-compressed image. They derived a blocking artifact characteristic matrix (BACM) for the JPEG images. In case of forgery, the regular symmetry of the BACM gets distorted and this can be used to validate the integrity of the images. Representation features from the BACM was used to train a support vector machine (SVM) classifier and recognize whether the image is an original JPEG image or it has been cropped from another JPEG image and re-saved. Mohammad et al. [27] in their paper present a novelmethod of DJPEG (the double JPEG) compression detection based on deep neural networks. Their paper detects DJPEG compression for small-sized 64 × 64 image patches. Furthermore, the approach identifies the regions that have been manipulated.

Another image forgery detection was proposed based on statistical correlations that appear in case of forgery [25]. Whenever a forger wants to make an impercetible forged image, she tries to stretch, resize or rotate the spliced portions of an image to fit properly into another image. This attempt to resample the forged image on a new sampling lattice introduces specific correlations. These correlations can be detected to authenticate or validate the integrity of the image and used for automatic detection of forged portion. This scheme was applicable only to the uncompressed TIFF, JPEG, and GIF images with minimal compression.

Another image forgery detection scheme based on Faster R-CNN model was proposed in [31]. They combined Laplacian of Gaussian (LoG) operator and Prewitt operator to detect edges and perform an end-to-end training. It gave satisfactory results for images manipulated with the addition of Gaussian white noise, Gaussian smoothing, and JPEG compression. However, it failed for post-processed images like smoothing the boundary traces between forged and unforged regions.

Zhou et al. [33], proposed a two-stream Faster R-CNN network to extract features that can help distinguish between forged and authentic images. First stream was based on RGB that extracted features based on strong contrast difference, unnatural tampered boundaries, etc. The second was a noise stream focused on leveraging the noise features and chalk out any inconsistency between the authentic and the tampered regions. The fusion of these streams was then coupled with a bilinear pooling layer to further incorporate spatial co-occurrence of these two modalities. It outperformed many state-of-the-art techniques for NIST Nimble 2016, COVER, CASIA, and the Columbia datasets.

Shubham et al. [17] proposed a robust, highly accurate, reduced feature-based algorithm detecting forged areas. In their proposed scheme, stationary wavelet transform is employed on the subject image to obtain a low approximation band, and then significant features are extracted using block-based. Salloum et al. [28] proposed another tampering localization technique by developing a framework that can learn boundaries of the spliced region, and the ground truth mask. The authors used a Multi-task Fully Convolutional Network for their experiments and found satisfactory results.

In [3], an algorithm based on SE-MinCut segmentation was proposed to extract the ghost borders. The Bhattacharyya distance was computed to calculate the distance between the original and the tampered regions, which was then fed into the classifier. Although, the automation of ghost detection was solved, but it cannot overcome the problem of low quality ghost-high quality cover image as mentioned in [9].

Here, we propose a robust image tamper detection scheme that works efficiently for all possible combinations of JPEG quality for ghost and cover images.

3 The proposed method

In the proposed method, we present a framework that can be used to verify the integrity of a dubious image as shown in Fig. 1. The method exploits the properties of the JPEG compression to detect the forgery in the images and also localize the tampered regions. Following are the detailed steps:

Step 1: Dubious image: A dubious image is a forged image that is obtained by copy pasting one portion of the image on another portion within the same image but saved at different JPEG qualities. For example, a central portion 50 by 50 of an image with a JPEG quality 60 called as ghost image, pasted on the cover image originally at quality 90. Different scenarios of the forgery of the image is discussed in detail in the experiment Section 4.

Step 2: Resave at different quality: To check the integrity of the dubious image, it is resaved at different JPEG qualities. We can done this for a range of [30, 100] with a step size of 2.

Step 3: RGB to YCbCr conversion: RGB color space is changed to YCbCr. Alteration in HVS is more sensitive to brightness changes as compared to color changes. The Y channel holds the luminance information of the image and the color information is contained in Cb and Cr channels. The dubious image I as well the resaved dubious image I^q are converted to YCbCr color space using the following:

$$\begin{aligned}\mathrm{Y} &= 0.257R + 0.504\mathrm{G} + 0.098B + 16\\ Cb &= -0.148\mathrm{R} - 0.291G + 0.439\mathrm{B} + 128\\ \mathrm{Cr} &= 0.439R - 0.368\mathrm{G} - 0.071\mathrm{B} + 128\end{aligned} \tag{1}$$

Step 4: Difference in energy: The difference image D is obtained by computing the absolute between the dubious image I and the resaved dubious image I^q and amplifying the difference as follows:

$$D(x, y) = \left[\mathrm{abs}(I(x, y)_i - I(x, y)_i^q)\right]_{i=1,2,3}^3 \tag{2}$$

where $I(x, y)_i$ and $I(x, y)_i^q$ represents the pixel value at (x, y) co-ordinates of the i^{th} color channel of the dubious image and resaved dubious image respectively. Here, the i^{th} value represents the Y, Cb and Cr channels respectively.

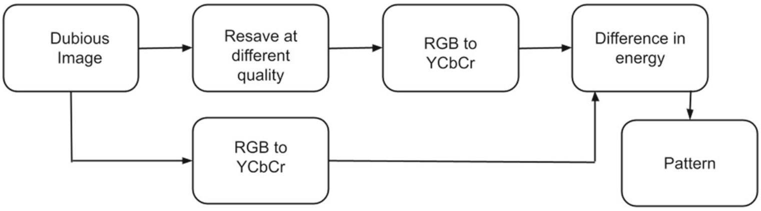

Fig. 1 An overview of the proposed methodology

Step 5: Pattern: To visualize the forged regions clearly, the difference image D is converted to binary, where the black and white regions represent the untampered and tampered portions of the image.

4 Experiment results

To validate the efficacy of the proposed method, we conducted different experiments on a standard dataset. A variety of attack scenarios were considered for the forgery, keeping the ghost image and the cover image at different JPEG qualities. Based on the results, we can say that the proposed method works efficiently in chalking out the tampered regions even for a high ghost image quality and low cover image quality as well as low ghost image quality and high cover image quality.

4.1 Dataset

The Uncompressed Color Image Database (UCID) is used to validate the experiments for the proposed method [29]. It contains high-quality TIFF images, some of which are shown in Fig. 2. We have created a database of JPEG images using the images of the UCID database. Firstly, all the 886 images of indoor and outdoor scenes of this database of size 512 × 384 or 384 × 512 is converted to JPEG format. Thereafter, we have made composite images by saving a portion of the image called as ghost image at a different JPEG quality and putting it back into the cover image and resaving the composite image at JPEG quality 100. The range of JPEG qualities that we have considered for the ghost and the cover image is in the range of $\{40, 45, 50, 55, \ldots\ldots, 85, 90, 95, 100\}$. Combinations of ghost-cover image are organized into multiple folders as follows:

We have 11 folders $F_{c_i g_j}$, where c and g represent the cover image and ghost image with i and j as their JPEG qualities. The values range for i and j falls into $i = \{40, 45, 50, 55, \ldots, 85, 90, 95\}$ and $j = \{40, 45, 50, 55, \ldots, 85, 90, 95, 100\}$. Each folder $F_{c_i\text{-}g_j}$ again contains 12 sub-folders $Z_{c_i\text{-}g_j}$, where c_i is kept constant and quality of ghost g_j is varied for all possible combinations. Hence, each sub-folder contains 886 × 12 composite images. Every image in the sub-folder is named as $xx\_yy\_zz.jpg$, where xx represents

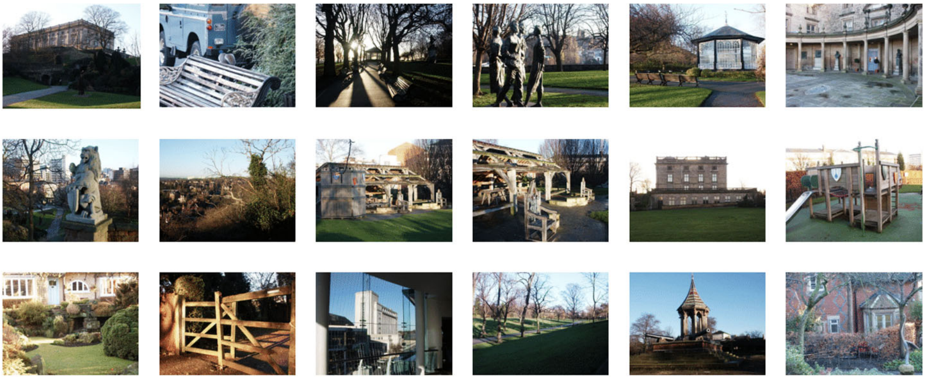

Fig. 2 Some representative images from the UCID dataset

the image number, yy implies the ghost image quality, and *zz* communicates the the cover image quality. In total, it contributes a dataset of 886 × 12 × 11 = 1,16,952 images.

Apart from this, we also considered attacks like inserting text into images, re-scaling the ghost images. For scale up attack scenarios, we increased 2 to 3 times and for scale down, we reduced the ghost image upto 1.5 times. Also, to test the detection accuracy of the forgery, we tested for ghost image size as small as 10 × 10 pixels.

4.2 Experiment scenarios

The experiments were conducted on a machine with Intel(R) Core(TM) i7-10750H CPU @2.60GHz, 64-bit processor, and 16GB RAM with Nvidia GeForce RTX 2060 on MATLAB R2020b. We have considered varied experiment scenarios for maximum possibilities of attack scenarios. For ghost image and cover image composite, we tested all combinations i.e. high quality of ghost image and low quality of cover image, low quality of ghost image and high quality of cover image, and ghost image and cover image both at the same quality. Other attack scenarios also like copy-move forgery, inserting text into image, rescaling (zoom-out/zoom-in) ghost image and then pasting on cover image. We also checked the proposed method for it's ability to detect even very small portions of forgery i.e. considering 50 × 50, 40 × 40 and going upto 10 × 10 pixel-sized forgeries.

The details of each of the experiment scenario along with the supporting results are briefed as follows:

1. The first scenario involves having a ghost image of higher image quality concerning that of the cover image. Results for some images considering it are shown in Fig. 3. This scenario arises when we download the images from social media sites or Apps that compresses the image, then the quality of this image lower than the real camera image. The attacker makes the forged image after downloading the image from social media application or compressed image.
    (a) In Grass field image, Cover image quality-65 and ghost image quality-85 of size 64 × 64 inserted at coordinate (190, 60).
    (b) In stair image, Cover image quality-90 and ghost image quality-55 of size 64 × 64 inserted at coordinate (190, 60).

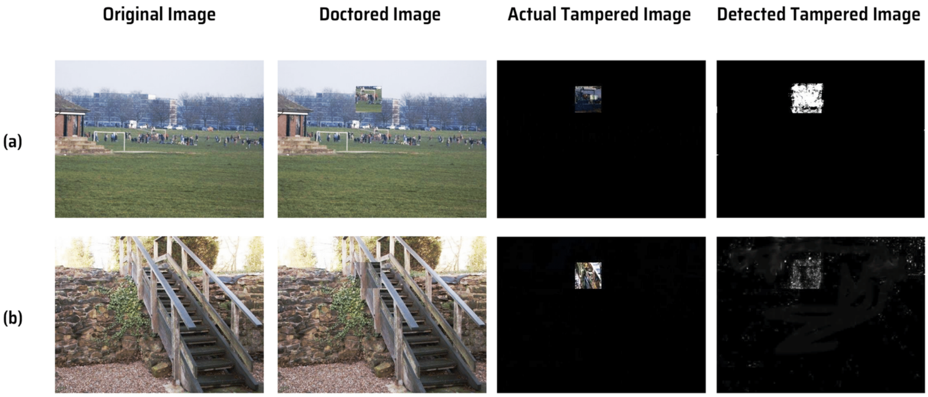

Fig. 3 Results of high quality ghost image inserted into low quality cover image (a) Grass field, (b) Stair

2. The second scenario involves having the ghost image of a lower image quality when compared to that of the cover image. Results for some images considering it are shown in Fig. 4.

   (a) In man image, Cover image quality-90 and ghost image quality-70 of size approx. 89 × 245 inserted at coordinate (190, 60).

   (b) In house image, Cover image quality-70 and ghost image quality-50 of size 64 × 64 inserted at coordinate (190, 60).

3. In the third scenario, both the cover image and the ghost image have the same quality. It may be both ghost and cover image compressed at some quality. Results for some images considering it are shown in Fig. 5.

   (a) In wall image, Cover image quality-75 and ghost image quality-75 inserted at coordinate (190, 60) of size 64 × 64.

   (b) In tree image, Cover image quality-45 and ghost image quality-45 inserted at coordinate (190, 60) of size 64 × 64.

4. In this scenario, the ghost image and cover image are the same quality because it is originally a part of the cover image and copied and pasted in the same cover image. Results for some images considering it are shown in Fig. 6.

   (a) In wall image, Cover image quality-45 and ghost image quality-45 of size 64 × 64 inserted at coordinate (190, 60).

   (b) In field image, Cover image quality-55 and ghost image quality-55 of size 30 × 68 inserted at coordinate (398, 170).

5. In this scenario, Inserting text into the cover image shows that the organisation's property or person. In this scenario, we cover the inserting text into image forgery detection, as shown in Fig. 7.

   (a) In the road image, the cover image's quality is 85, and it contains text, i.e., "Hello MATLAB!" at coordinate (197,243) of size 10.

   (b) In the glass image, the cover image's quality is 75, and it contains text, i.e., "Abcd" at coordinate (248,192) of size 14.

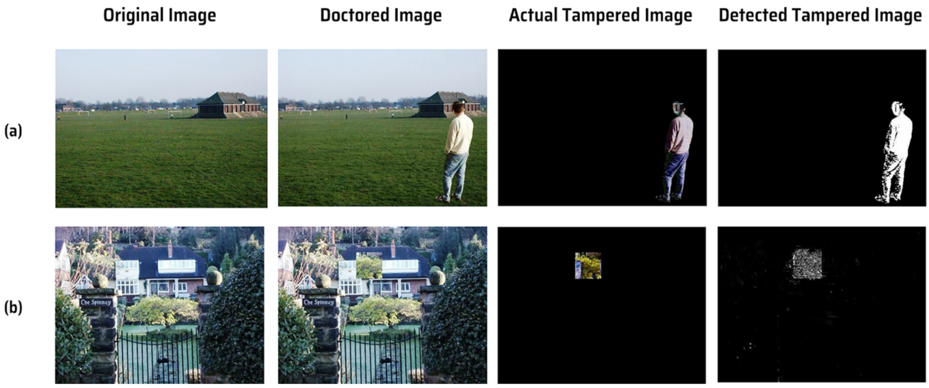

Fig. 4 Results of low quality ghost image inserted into high quality cover image (a) Man, (b) House

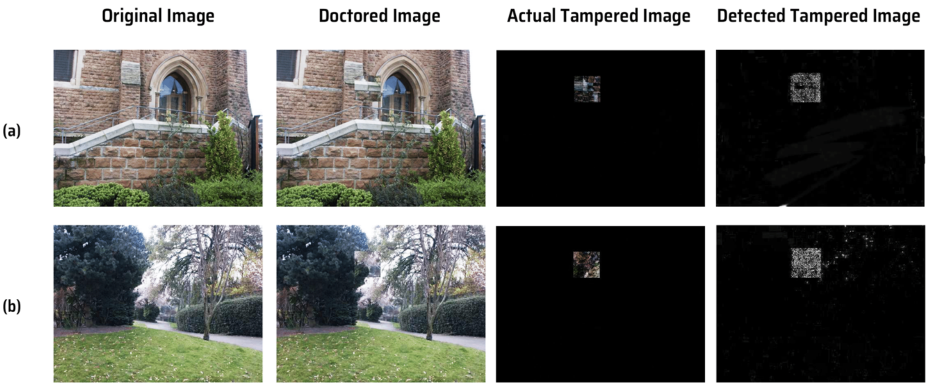

Fig. 5 Results of both the image (Ghost and cover image) quality is same. (a) Wall, (b) Tree

6. The sixth scenario involves taking portions of the cover image as the ghost images and resizing them (zoom out/in). Zoom out/in means enlarging/reducing the size of a picture in a sense and pasting them onto the cover image. Results for some images considering it are shown in Fig. 8.
   (a) In the house image, the cover image's quality is 65, and it contains a windows picture in the zoom-out form at coordinate (359,102) of size 62 × 37 to 105 × 76.
   (b) In the tiger image, the cover image's quality is 40, and it has a copy of the tiger in the zoom-in form at coordinate (352,183) of size 240 × 160 to 148 × 87.
7. In this scenario. the ghost image size is kept 10x10, 20X20, 30X30, 40x40, 50x50, 60x60 pixels in the cover image to detect the adulteration. Results for some images considering it are shown in Fig. 9. In this experiment, we show how small the size of the ghost image can be detected / visible.
   (a) In the sliding image, the cover image's quality is 85, and ghost image quality 65 at coordinate (29,9) of size 10 × 10.
   (b) In the wood-house image, the cover image's quality is 85, and ghost image quality 65 at coordinate (89,28) of size 30 × 30.

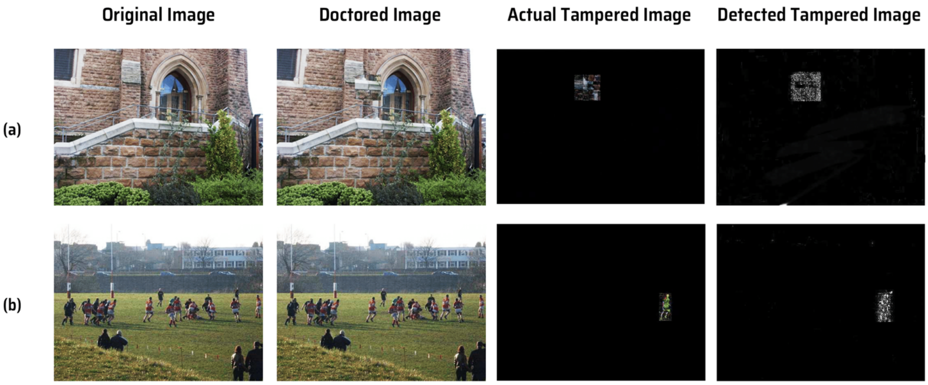

Fig. 6 Results of copy and paste the portion of image into same image. (a) Wall, (b) Field

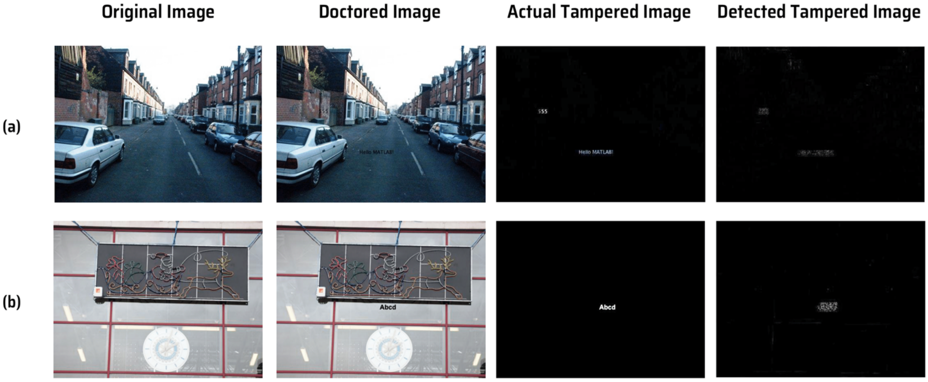

Fig. 7 Results of inserting text into image. (a) Road, (b) Glass

We analyzed the different combinations of ghost and cover image by varying the JPEG quality for the resaved composite images. Based on the experiments and testing with a sufficiently large dataset, we found that the detection of the forged regions is good for a range of JPEG quality compared to the entire range and possible combinations for ghost and cover images. We exploited SSIM [12] to measure the similarity between a forged image I and it's corresponding resaved version I^q at a quality q using following:

The SSIM formula is based on three comparison measurements between the samples of I and I^q: luminance (l), contrast (c) and structure (s). The individual comparison functions are:

$$\text{SSIM}(I, I^q) = [l(I, I^q)] \cdot [c(I, I^q)] \cdot [s(I, I^q)] \tag{3}$$

where

$$l(I, I^q) = \frac{2\mu_I \mu_{I^q} + C_1}{\mu_I^2 + \mu_{I^q}^2 + C_1} \tag{4}$$

$$c(I, I^q) = \frac{2\sigma_I \sigma_{I^q} + C_2}{\sigma_I^2 + \sigma_{I^q}^2 + C_2} \tag{5}$$

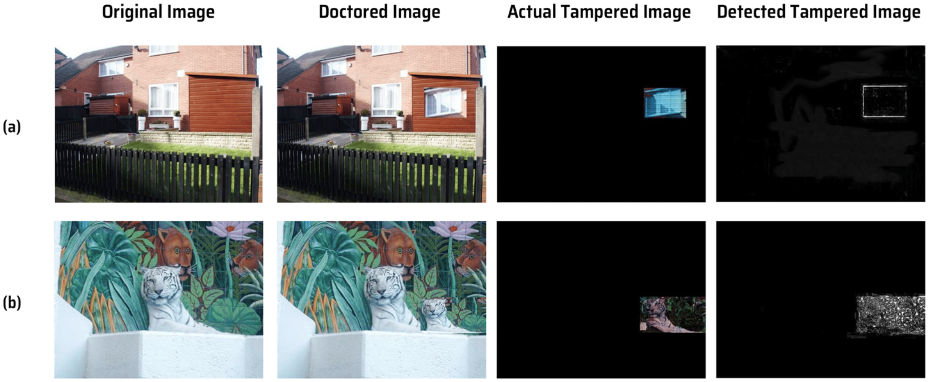

Fig. 8 Results of Rescale (Zoom-in / Zoom-out) an object in the image. (a) House, (b) Tiger

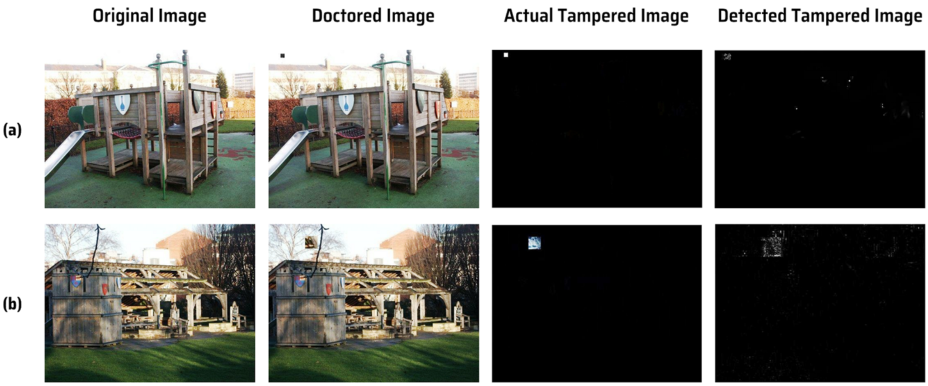

Fig. 9 Results of JPEG ghost block size 10 × 10 and 30 × 30. (a) Sliding, (b) wood-house

$$s(I, I^q) = \frac{\sigma_{II^q} + C_3}{\sigma_I \sigma_{I^q} + C_3} \tag{6}$$

Here, μ_I is the average of I, μ_{I^q} is the average of I^q , σ_I^2 is the variance of I , $\sigma_{I^q}^2$ is the variance of I^q, σ_{II^q} is the covariance of I and y, $c_1 = (k_1 L)^2$, and $c_2 = (k_2 L)^2$ are two variables to stabilize the division with weak denominator, L is the dynamic range of the pixel-values, $k_1 = 0.01$, $k_2 = 0.03$, and $c_3 = \frac{c_2}{2}$.

By analyzing plots of “SSIM value” versus “compression quality factor” of the resaved image, we found that the first maxima occurs at values near the original quality of the cover image as shown in Fig. 10a. Here, the first maxima occurs at 50 JPEG quality which was also the quality of the the cover image.

We performed another analysis for the experiment scenarios based on the difference in energy of the forged and it’s resaved version using (7).

To calculate energy of image-

$$E(x, y) = \sum_{d=1}^{dim} \sum_{x=1}^{rows} \sum_{y=1}^{col} D(x, y, d) \tag{7}$$

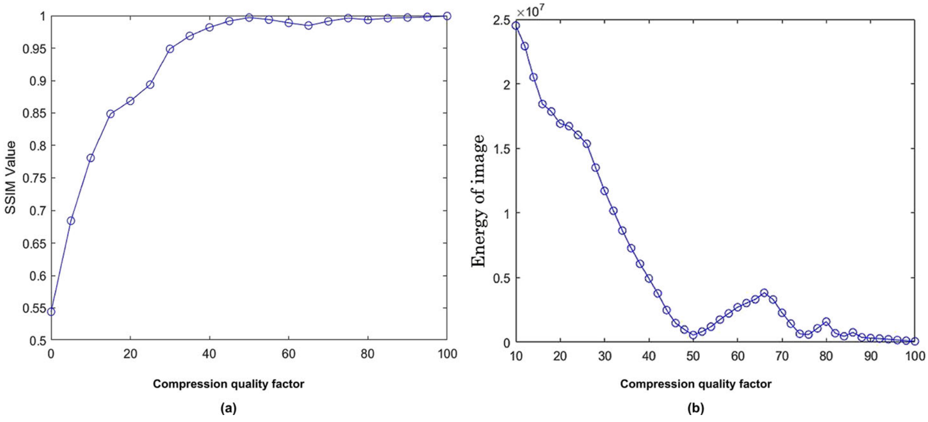

Fig. 10 (a) SSIM Graph (b) Energy Graph

where $E(x, y)$ represents the sum of the amplified pixel values $D(x, y)_i$ of the difference image obtained in (2).

The first minima in plots of “energy of image” versus “compression quality factor” correspond to the quality of the cover image quality. For instance, the first minima in Fig. 10b occur at compression quality 50, which again corresponds to the quality of the cover image. Hence, this cross-verifies the result that we obtained using SSIM plots.

4.3 Comparison table

A comparative study of the proposed scheme with the other state-of-the-art tamper detection approaches based on various criteria has been tabulated in Tables 1 and 2. A few of the criteria are described as follows:

- **Blind authentication**: If the integrity of an image can be checked just based on the content of the given image without any additional information or attributes, it is termed as blind authentication.
- **Is detection possible with just one image?**: This criteria is based on whether the forgery detection can be done with just a single available image or a bunch of images are needed to detect the forged regions. For example, detection based on Photo Response Non-Uniformity (PRNU) of a camera.
- **Can the technique detect very minute forgeries?**: This criteria is based on what level of forgery detection can be done by a scheme. We are referring to forgeries less than 10 × 10 sized pixels as the minute forgeries.
- **Can the technique predict quality of the original image?**: This criteria is based on whether an algorithm can predict the JPEG quality of the original cover image or not.

  The proposed scheme can narrow down this range of possible JPEG quality and can detect in very less iterations.
- **JPEG quality**: In this type of forgery, the content of an image at JPEG quality q_1 is copied and pasted into another image of JPEG quality q_2. This composite image is then resaved at different JPEG qualities and forgery detection is performed based on these quality differences.
- **Copy-move**: In this type of forgery, a portion of an image is copied and pasted into another place in the same image to hide other information or falsify the original content of the image.
- **Text insertion**: In this type of attack, some text messages are inserted on top of the original content of the image.
- **Rescale**: In this type of attack, few portions of the original image are rescaled (ZoomIn/ZoomOut) and pasted over to conceal some important information in the original image to falsify the information.

From Tables 1 and 2, we can observe that only two schemes proposed in [22, 32] cannot do the blind authentication. They require additional information. Sharing phase of [32], a secret image is encoded into shared bits by polynomial based secret image sharing. Source linkage based on header information of media items allow for easy automation in [22]. In general, detection of forged regions based on just a single image becomes quite challenging. Hence it is an important criteria to judge usuability of a proposed scheme. This is possible for all the schemes considered for comparison here except for [13]. Hou et al. [13] needs to achieve this goal, we use sensor pattern noise from each color channel of untampered

Table 1 Comparison based on various criteria

	Blind authentication	Is detection possible with just one image?	Can detect very minute forgeries	Can predict quality of original image
Wu et al. [32]	No	Yes	Yes	No
Thai et al. [30]	Yes	Yes	Yes	Yes
Hou et al. [13]	Yes	No	No	No
Chierchia et al. [6]	Yes	Yes	No	No
Agarwal et al. [1]	Yes	Yes	–	No
Azarian et al. [3]	Yes	Yes	Yes	Yes
Kumawat et al. [18]	Yes	Yes	–	No
Pun et al. [26]	Yes	Yes	Yes	No
Chen et al. [5]	Yes	Yes	Yes	No
Mullan et al. [22]	No	Yes	–	No
Bhardwaj et al. [4]	Yes	Yes	–	Yes
Proposed Scheme	Yes	Yes	Yes	Yes

Table 2 Comparison based on various attack scenarios

	JPEG Quality	Copy-move	Text Insertion	Rescale
Wu et al. [32]	No	No	No	No
Thai et al. [30]	Yes	Yes	No	No
Hou et al. [13]	Yes	No	No	No
Chierchia et al. [6]	No	Yes	No	No
Agarwal et al. [1]	Yes	Yes	Yes	No
Azarian et al. [3]	Yes	No	No	No
Kumawat et al. [18]	No	No	No	No
Pun et al. [26]	–	Yes	No	No
Chen et al. [5]	No	Yes	No	No
Mullan et al. [22]	No	Yes	–	No
Bhardwaj et al. [4]	–	–	No	No
Proposed Scheme	Yes	Yes	Yes	Yes

images as the ground truth. The level of forgery detection is very crucial for sensitive applications. Forgeries as minute as 10 × 10 sized blocks can cause a lot of damage for critical applications. The proposed scheme is capable to detect such minute forgeries. Many forgery detection schemes become computation expensive as they have to repeat the entire process again and again to detect the forged regions. One such forgery detection is based on JPEG qualities. If it is possible to predict the original quality of the JPEG image, then this process can be accelerated. In the proposed scheme, the quality of the original image can be predicted using the SSIM and energy graphs. Agarwal and Farid [1], Azarian-Pour et al. [3], Hou et al. [13], and Thai et al. [30] schemes can detect forgery based on difference of JPEG quality in the cover and the ghost image.

Varied attack scenarios such as attacks based on JPEG quality, copy-move forgery, insertion of text into images and rescaling a portion for falsifying the original information are considered to evaluate the performance of the proposed scheme. Table 2 enlists the attack scenarios. The state-of-the-art schemes are compared based on their robustness towards these scenarios. The proposed scheme can tackle all the aforementioned attacks.

5 Conclusion and future research directions

This paper describes an effective technique for detecting tampering in JPEG images. Based on the experiments, we have observed that if two different images of different JPEG qualities are combined to obtain a composite image, the possibility of detecting the forgery is quite high. Based on the study in the experiments, the quality of the cover image can be predicted based on the “SSIM” and “energy of image” verses “compression quality factor” plots.

The proposed approach helps in reducing a lot of efforts needed to detect the tampered portion as well, as one can directly check the narrow range near the maxima/minima points in the SSIM/Energy plots. However, if the two combined images have the same JPEG quality, the detection possibility becomes quite low. This is irrespective of the fact whether the images were captured from the same camera device or not. The future directions could be localizing the forgery in images that have undergone multiple compressions. Another research direction could be localizing the forged area of images with multiple forgeries.

Funding There are currently no funding sources for this work.

Declarations

Conflict of interest/Competing interests The authors declare that there is no actual or potential conflict of interest regarding the publication of this article.

References

1. Agarwal S, Farid H (2017) Photo forensics from jpeg dimples. In: 2017 IEEE Workshop on information forensics and security (WIFS). IEEE, pp 1–6
2. Avcibas I, Bayram S, Memon N, Ramkumar M, Sankur B (2004) A classifier design for detecting image manipulations. In: 2004 International conference on image processing, 2004. ICIP’04, vol 4. IEEE, pp 2645–2648

3. Azarian-Pour S, Babaie-Zadeh M, Sadri AR (2016) An automatic jpeg ghost detection approach for digital image forensics. In: 2016 24th Iranian conference on electrical engineering (ICEE). IEEE, pp 1645–1649
4. Bhardwaj D, Pankajakshan V (2018) A jpeg blocking artifact detector for image forensics. Signal Process: Image Commun 68:155–161
5. Chen C-C, Lu W-Y, Chou C-H (2019) Rotational copy-move forgery detection using sift and region growing strategies. Multimed Tools Applic 78(13):18293–18308
6. Chierchia G, Poggi G, Sansone C, Verdoliva L (2014) A bayesian-mrf approach for prnu-based image forgery detection. IEEE Trans Inf Forensics Secur 9(4):554–567
7. Express NI Malaysian politician faked photo of knighthood, https://www.newindianexpress.com/world/2010/. Accessed 30 March 2020
8. Fake news alert! 15 hoax stories that people almost believed in 2017, https://indianexpress.com/article/trending/trending-globally/ (2017). Accessed 30 March 2020
9. Farid H (2009) Exposing digital forgeries from jpeg ghosts. IEEE Trans Inform Forens Secur 4(1):154–160
10. Fridrich AJ, Soukal BD, Lukáš AJ (2003) Detection of copy-move forgery in digital images. In: Proceedings of digital forensic research workshop. Citeseer
11. Garcia L 5 quick ways we can all double-check coronavirus information online, https://firstdraftnews.org/. Accessed 30 March 2020
12. Hore A, Ziou D (2010) Image quality metrics: Psnr vs. ssim. In: 2010 20th international conference on pattern recognition. IEEE, pp 2366–2369
13. Hou J-U, Jang H-U, Lee H-K (2014) Hue modification estimation using sensor pattern noise. In: 2014 IEEE International conference on image processing (ICIP). IEEE, pp 5287–5291
14. Jarusek R, Volna E, Kotyrba M (2019) Photomontage detection using steganography technique based on a neural network. Neural Netw 116:150–165
15. Johnson MK, Farid H (2006) Exposing digital forgeries through chromatic aberration. In: Proceedings of the 8th workshop on multimedia and security, pp 48–55
16. Johnson MK, Farid H (2007) Exposing digital forgeries in complex lighting environments. IEEE Trans Inf Forensics Secur 2(3):450–461
17. Kumar S, Mukherjee S, Pal AK (2022) An improved reduced feature-based copy-move forgery detection technique. Multimed Tools Applic, 1–26
18. Kumawat C, Pankajakshan V (2020) A robust jpeg compression detector for image forensics. Signal Process: Image Commun 89:116008
19. Lukáš J, Fridrich J, Goljan M (2006) Detecting digital image forgeries using sensor pattern noise. In: Security, steganography, and watermarking of multimedia contents VIII, vol 6072. International Society for Optics and Photonics, p 60720
20. Luo W, Qu Z, Huang J, Qiu G (2007) A novel method for detecting cropped and recompressed image block. In: 2007 IEEE International conference on acoustics, speech and signal processing-ICASSP'07, vol 2. IEEE, p 217
21. Malathi J, Nagamani TS, Lakshmi KNVSKV, devi PR (2019) Survey: image forgery and its detection techniques. J Phys Conf Ser
22. Mullan P, Riess C, Freiling F (2019) Forensic source identification using jpeg image headers: the case of smartphones. Digit Investig 28:68–S76
23. Ng T-T, Chang S-F (2004) A model for image splicing. In: 2004 International conference on image processing, 2004. ICIP'04, vol 2. IEEE, pp 1169–1172
24. Popescu AC, Farid H (2004) Exposing digital forgeries by detecting duplicated image regions. Dept. Comput. Sci., Dartmouth College, Tech Rep TR2004-515, 1–11
25. Popescu AC, Farid H (2005) Exposing digital forgeries by detecting traces of resampling. IEEE Trans Signal Process 53(2):758–767
26. Pun C-M, Yuan X-C, Bi X-L (2015) Image forgery detection using adaptive oversegmentation and feature point matching. IEEE Trans Inf Forensics Secur 10(8):1705–1716
27. Rahmati M, Razzazi F, Behrad A (2022) Double jpeg compression detection and localization based on convolutional auto-encoder for image content removal. Digit Signal Process 123:103429
28. Salloum R, Ren Y, Kuo C-CJ (2018) Image splicing localization using a multi-task fully convolutional network (mfcn). J Vis Commun Image Represent 51:201–209
29. Schaefer G, Stich M (2003) Ucid: an uncompressed color image database. In: Storage and retrieval methods and applications for multimedia 2004, vol 5307. International Society for Optics and Photonics, pp 472–480
30. Thai TH, Cogranne R, Retraint F et al (2016) Jpeg quantization step estimation and its applications to digital image forensics. IEEE Trans Inf Forensics Secur 12(1):123–133

31. Wei X, Wu Y, Dong F, Zhang J, Sun S (2019) Developing an image manipulation detection algorithm based on edge detection and faster r-cnn. Symmetry 11(10):1223
32. Wu X, Yang C-N, Yang Y-Y (2020) Sharing and hiding a secret image in color palette images with authentication. Multimed Tools Applic 79(35):25657–25677
33. Zhou P, Han X, Morariu VI, Davis LS (2018) Learning rich features for image manipulation detection. In: Proceedings of the IEEE conference on computer vision and pattern recognition, pp 1053–1061

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.