An Exploration of Digital Image Forensic Techniques: A Brief Survey

Divya P. Surve and Anant V. Nimkar

Abstract Digital image forensics deals with assessing whether an image is genuine or not. As an image may undergo several manipulations done to either improve its quality or to intentionally change its meaning it is very difficult to conclude if an image is forged or is genuine. In this paper, three important aspects of image forgery detection are explored. An in-depth discussion of image forgery detection, a technique which is based on assessing image features categorized under active and passive methods is present. Analysing both image features and device features to know the image capturing device while checking for forgery is explained in detail. Provenance analysis which is the entire derivation of image manipulation history is also expressed. Discussion regarding research directions in the domain of image forensics is mentioned in the paper.

Keywords Image forgery detection · Illumination estimation · Image source camera identification · Image provenance analysis

1 Introduction

Digital images are a great medium for conveying information through various communication mediums. Easy manipulation of images due to advance image editing tools leads to change in message sent. Image forgery detection or image manipulation detection identifies such manipulation done in the images in order to change its meaning.

Image forgery detection is a multi-faceted approach having multiple viewpoints. There are various active and passive methods to detect image forgery based on image features. Illumination direction estimation is a technique under passive image forgery detection. Image source camera identification is an important area where features of

D. P. Surve (✉) · A. V. Nimkar
Sardar Patel Institute of Technology, Mumbai, India
e-mail: divya.surve@spit.ac.in

A. V. Nimkar
e-mail: anant_nimkar@spit.ac.in

U. P. Rao et al. (eds.), *Security, Privacy and Data Analytics*, Lecture Notes
in Electrical Engineering 1049, https://doi.org/10.1007/978-981-99-3569-7_3

both capturing device and images are analysed to know the source of an image [3]. Image provenance analysis builds a graph wherein the series of manipulation for an image is derived [9].

This review addresses the various concerns in detecting forgery by means of illumination-based technique which is a method under passive image forgery detection. In image forgery detection and source device identification, this paper focuses on devising mechanism that can distinguish well between genuine image enhancement operations of scaling, rotation with those of image manipulation operations well. In case of provenance analysis, this paper tries to show the importance of dealing with near-duplicate images, donor images of small size and use of metadata information.

Considering environmental lighting conditions is one possible alternative to the problems under passive physics-based method of image forgery detection. Image forgery detection with source camera identification giving equal importance to forgery detection and genuine manipulation detection is discussed in the paper. Techniques to deal with donor images of small sizes and near-duplicate images using contextual masks, metadata information, etc. is highlighted in the paper.

In order to experiment with issues in illumination-based forgery detection, distinguished object in an image needs to be identified. Illumination direction should be estimated for these objects including the background of an image. For dealing with the problem of having perceptual robustness, techniques for genuine image manipulation detection need to be experimented first before hash computation. For faster provenance analysis, metadata of an image database can be considered.

Our significant contribution in the domain of image forgery detection are as follows:

- Detailed discussion of the areas in digital image forgery detection which are active/passive forgery detection techniques, image forgery detection with source camera identification and image provenance analysis.
- Minutely stated problems related to all the three domains of passive illumination-based image forgery detection, image source device identification and provenance analysis.
- Possible solutions to the stated problems are also discussed in the paper.

The paper is organized as follows: Sect. 2 states background of the domain explaining basic terminologies and techniques under digital image forensics which are image forgery detection, image forgery detection with source device identification and provenance analysis. Section 3 discusses the motivation and related work, Sect. 4 discusses the various issues in three areas mentioned. Section 5 details possible area to explore in the area of digital image forensics. Section 6 states conclusion regarding learning derived from the overall review on digital image forensics. Section 7 discusses the future possible areas to explore in the domain of image forensics.

2 Background

The domain of digital image forensics has three important aspects of:

1. Image forgery detection.
2. Image forgery detection with source camera identification.
3. Image provenance analysis.

2.1 Image Forgery Detection

Image forgery detection methods check for properties of an image to decide if an image is genuine or forged. Image forgery detection method depends on the image storage formats. The forgery detection method for image depends on the type of image and the format of compression of an image. A detail of strategies employed for detection of JPEG and PNG images is discussed in [15–18].

There are multiple active and passive image forgery detection methods which are employed. Active image forgery detection techniques rely on use of proactive measures like watermarking, digital signature and texture analysis to know presence of any forged content in an image [19, 25]. Passive image forgery detection techniques use measures like image features based on comparison of pixel values, compression methods, camera properties, illumination environment and geometric features [7, 25].

Image forgery detection technique involves the following six steps, namely, pre-processing, image feature extraction, image feature matching, false match removal, result optimization and region localization [7, 25]. The details of every phase are depicted below:

- Pre-processing: This operation enhances image quality to be useful in the further phases of processing. Operations like noise removal, resizing and colour-space conversion, segmentation, etc. are carried out to make it suitable for training.
- Image feature extraction: Unique distinguishable features are extracted from the image. These features represent values that are used as an identifier for image rather than the entire set of pixel values. It uses techniques of transformation based on coding, hashing, LBP method, key point processing and histogram-based processing.
- Image feature matching: Features extracted from the query image are matched with the features of images in the database. If the resultant value of matching formula computed over the query image is within acceptable range, then the image is considered to be genuine else some manipulation is said to have occurred. Some popularly used image feature matching techniques are nearest neighbour technique, clustering and segmentation, thresholding, Manhattan distance, etc.
- False match removal: If multiple matches are detected from the database for a given query image, then removal of the images which are falsely detected as matching is

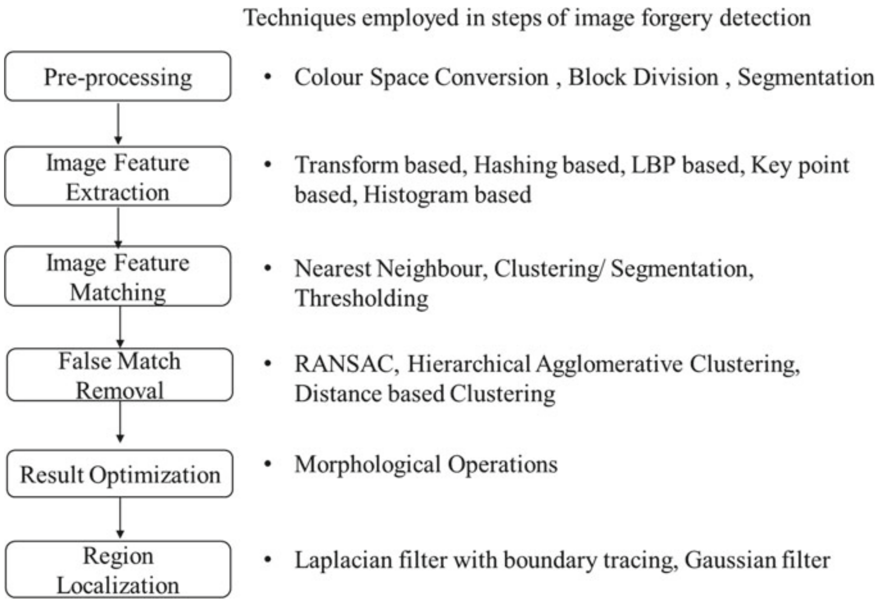

Techniques employed in steps of image forgery detection
Pre-processing
Image Feature Extraction
Image Feature Matching
False Match Removal
Result Optimization
Region Localization
• Colour Space Conversion , Block Division , Segmentation
• Transform based, Hashing based, LBP based, Key point based, Histogram based
• Nearest Neighbour, Clustering/ Segmentation, Thresholding
• RANSAC, Hierarchical Agglomerative Clustering, Distance based Clustering
• Morphological Operations
• Laplacian filter with boundary tracing, Gaussian filter

Fig. 1 Steps in image forgery detection

carried out in this phase. The techniques of RANSAC, hierarchical agglomerative technique and distance-based techniques are used to remove such false matches.

- Result optimization: The resultant images after removal of false match are passed through morphological operations to derive the structure of the forged content. It is used to optimize the resultant structure derived of the objects present in the image using operation of dilation, erosion, closing and opening operations.
- Region localization: Images derived from region optimization process are further processed in Region localization phase to get accurate boundaries of objects. Filters like Laplacian filter, Gaussian filter, etc. are used here to derive the boundary of the objects.

2.2 Image Forgery Detection using Source Camera Identification

Every digital image captured by a device will have properties as embedded by the capturing device. Set of images captured by a camera may induce distortion uniformly at same location in all images captured by that device. Such peculiar pattern of intensities can act as distinguishing feature of image source helping in identification of image forgery using source camera detection [1–6]. The features of colour filter array, photoresponse non-uniformity pattern [1], sensor pattern noise [1] and

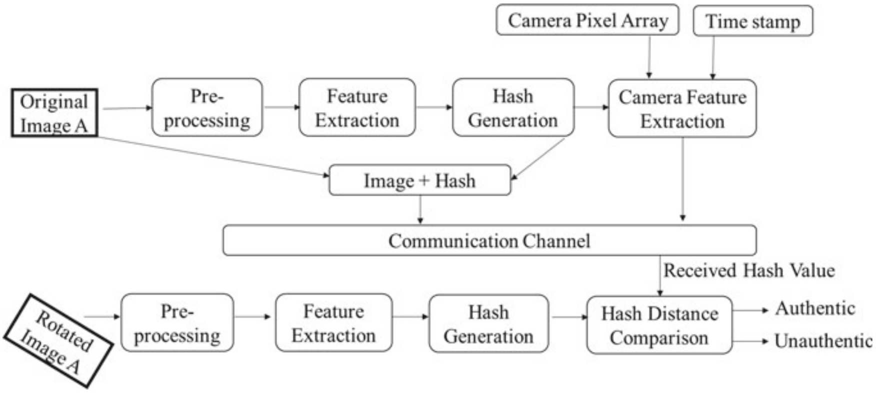


Fig. 2 Steps in image forgery detection with source device identification

compression scheme [5] are some of the features of the capturing device to check the type of device and the brand of it.

Image forgery detection with source camera identification involves the following phases as mentioned in [2, 3], namely, pre-processing, feature extraction, camera feature extraction, hash generation and hash distance comparison.

- Pre-processing: The image is checked to see if it is suitable for the further processing phases. If not operations of image enhancement are applied to make it apt for further phases of feature extraction.
- Feature Extraction: The aim here is to extract features from an image in order to identify image using minimum representative pixels. The extraction process can vary depending on the type of features to be extracted from the image.
- Camera Feature Extraction: Combined features from capturing device and image are extracted to have a minimum representative set of values for every image. Features include PRNU, SPN, colour filter array or compression scheme.
- Hash Generation: Hash value is generated using both the device features and the image features. The generated hash value is appended to the captured image and sent through the communication channel. A similar process in the reverse fashion is followed at the receiver's end.
- Hash Distance Comparison: If the generated hash value at the receiver's end is within the decided threshold then the image generated is said to be authentic else it is called to be tampered one.

2.3 Image Manipulation History Tracking

An image may undergo series of manipulation before it is ready to use for a particular application. In provenance analysis, identification of the entire set of contributing images for a given query image is carried out. This would ultimately help in under-

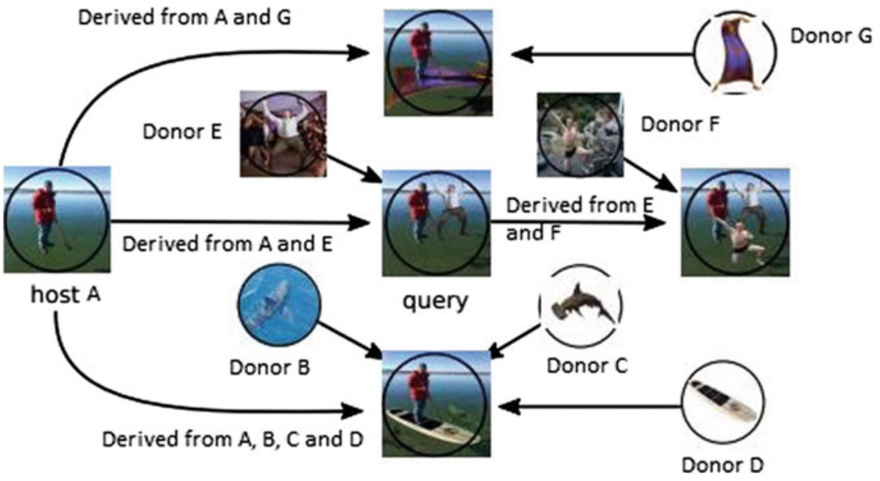
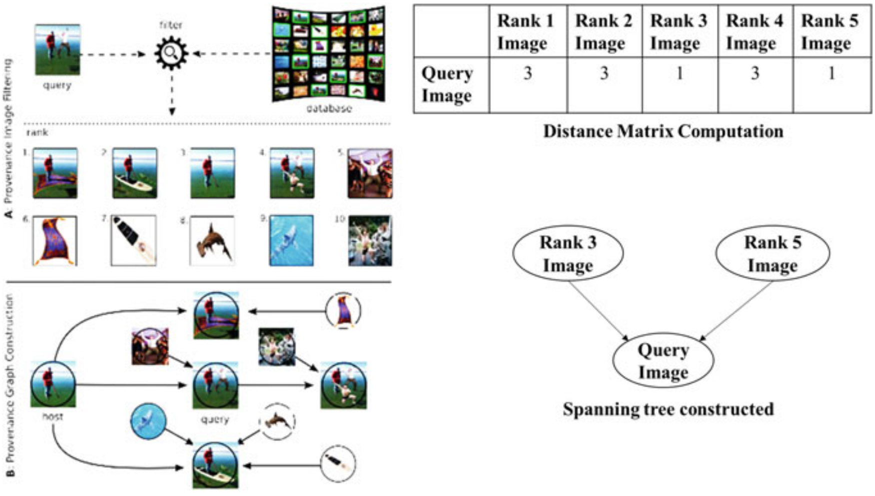


Fig. 3 Image source identification and provenance graph construction



	Rank 1 Image	Rank 2 Image	Rank 3 Image	Rank 4 Image	Rank 5 Image
Query Image	3	3	1	3	1

Distance Matrix Computation

Fig. 4 Steps in provenance analysis

standing the reason for manipulation in the query image. As shown in Fig 3, the central query image has donors from multiple images like image A and image E. Also multiple images can be derived from query image too. Hence, there can be a series of manipulation that an image can undergo. Figure 4 from [9] depicts detailed steps involved in provenance analysis:

- Provenance Image Filtering: A search for the extracted features from the query image and the database of images is carried out. The matched images are then ranked like in Fig. 4, so as to find the best suitable match in the database for the various objects present in the query image [9–11, 13, 14].

- Provenance Graph Construction: Once the images are filtered so as to find the best images from the database, a dissimilarity matrix is constructed between the query image and the best match images. This matrix is further converted to a graph using minimum spanning tree algorithm to get the history of manipulation for the query image [9, 10, 23, 24]. As depicted in Fig. 4, ten images having rank 1–10 are assessed during graph construction phase. The distance between query image and the top 5 best ranked images is mentioned in the matrix. Rank 3 image is the closest to the query image having maximum content derived from it and hence named as host image. Rank 5 image has some content adopted in the query image and has the next least distance from the query image. The query image is thereby derived from the Rank 3 and Rank 5 images, respectively. Similarly, in the distance matrix we can consider images till Rank 10 as well based on algorithmic thresholds placed.

3 Motivation and Related Work

This section provides an elaborate detail of various techniques under image forgery detection. A detailed comparison of techniques under image forgery detection with source device identification is provided for reference. Investigation of techniques under provenance analysis with varied donor sizes is also expressed.

In Table 1, details regarding various techniques under digital image forensics based on pixel values, compression method, camera properties, physics of lighting condition and geometric properties of image capturing device are mentioned.

Table 2 provides a comparison regarding various image forgery detection techniques based on source camera identification. Techniques here are compared based on parameters of perceptually robust operations of rotation and scaling. Other parameters of comparison are whether tamper detection, device authentication are possible. It can be observed that there is a need to attain better accuracy level where genuine image manipulation is well differentiated to that of tamper operation.

Table 1 Image forgery detection techniques

Techniques	Methods
Pixel based	Copy-Move, Splicing, Resampling, Retouching
Compression based	JPEG Quantization, Double JPEG, Multiple JPEG, JPEG blocking
Camera based	Chromatic Aberration, Source Camera Identification, Pixel Array, Sensor Noise
Physics based	2D and 3D Light Direction, Light Environment
Geometric based	Camera Intrinsic Parameters, Multi-view geometry

Table 2 Comparison of various image forgery detection techniques with image source identification

Techniques	Rotation	Scaling	Tamper detection	Device authentication
[4]	80.02	1	Yes	No
[1]	No	No	Yes	Yes
[2]	No	No	Yes	Yes
[3]	96.25	90.42	95.42	Yes

Table 3 Comparison of image provenance analysis techniques based on various size donors

Paper	SD	SDR	MD	MDR	LD	LDR
[9]	195	28.3	265	56.8	286	67.0
[28]	195	33.3	265	72.6	286	76.8
[23]	195	**55.3**	265	**75.2**	286	**78.0**

Table 3 [23] provides an analysis of various provenance analysis techniques proposed in [9, 23, 28]. The terms #SD, #MD and #LD mean count of small donor, medium donor and large donor. The terms SDR, MDR and LDR mean small, medium and large donor recall rate. The dataset MFC19EP1 is being considered for evaluating these parameters. Donor images having spliced region less than 1 percent of its image size are classified as small donors. Spliced images greater than 10% of its size are classified as large donor and the others are considered as medium size donors. Same number of samples under various categories of small, medium and large when compared attains a recall rate of around 78% for donors of large size, however it can attain only 55% of recall rate for small size donors. The observation is similar for other provenance-based datasets like MFC18EP1, MFC17EP1 and Reddit real time. This emphasizes the need to improve on detection of small spliced regions while building provenance graph.

4 Discussion

In this section problems associated with every image forgery detection scheme is discussed in depth.

4.1 Image Forgery Detection Using Illumination-Based Methods

Illumination-based methods of image forgery detection come under the category of physics-based methods for detection of fraud image. In [8, 21] technique, the illumination pattern of the objects in the scene is analysed to check if there is any false content present. The falsification could be because of splicing of multiple images or using small cropped objects from the same image. Detection of spliced objects based on colour illumination inconsistencies is discussed in [20]. In spliced images where there is a seamless integration of images present it is difficult to find the difference between the objects at the first glance. However, analysing them thoroughly using methods of illumination detection can reveal such forged content.

Figure 5 from [8] gives a good example of illumination direction estimation for forgery detection. There are two parts in the image where the top image is the coloured image seamlessly spliced from multiple source. The bottom part is the illumination estimated for the image on top. If observed carefully one can see in the bottom black and white image that the dominant illumination direction estimated for two people on the left is towards left while for the three people on the right is towards right. Hence, analysing the illumination pattern of objects in a scene provides a good intuition about image forgery. However, there exists certain area of concerns in such methods as stated below:

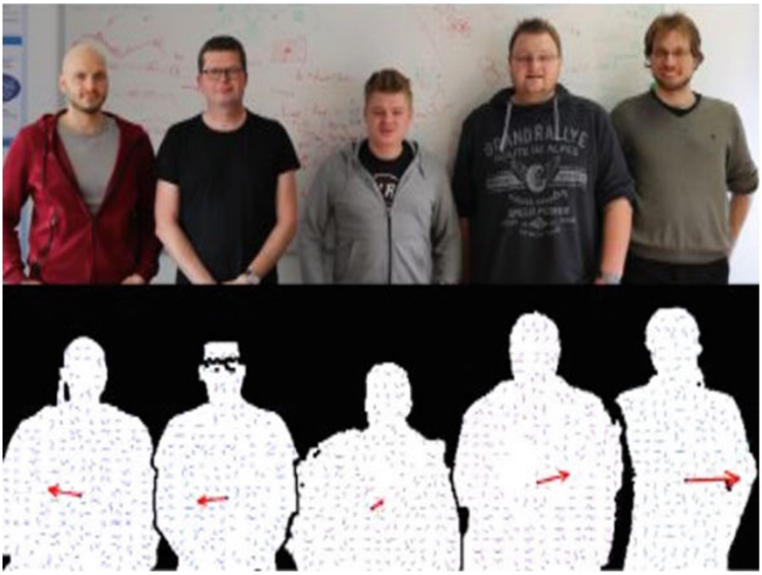


Fig. 5 Illumination direction estimation of scene objects [8]

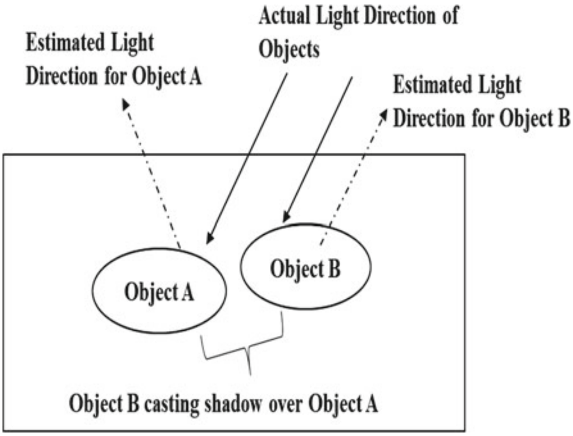

Estimated Light Direction for Object A
Actual Light Direction of Objects
Estimated Light Direction for Object B
Object A
Object B
Object B casting shadow over Object A

Fig. 6 Incorrect Illumination direction estimation due to shadow effect

- Incorrect illumination direction estimation due to shadow effect:
  An incorrect estimation of source light occurs when objects in the scene cast their shadow over the other objects present leading to a misinterpretation that these objects are illuminated by different light sources but in actual they might be illuminated from the same source itself. Consider Fig. 6, where an image has two objects A and B, they are illuminated by the same light source shown by plain arrow and their estimated light directions in dashed arrow. However, object B casts its shadow on object A which changes the illumination direction estimation of object A. Even though objects A and B belong to the same image they are concluded to belong to different images and are forged. Hence, appropriate estimation of illumination direction considering the effect of shadow from objects becomes important.
- Incorrect illumination direction estimation due to multiple spliced objects from same source:
  A spliced image is generated using image from different source. Two objects copied and pasted from same source and pasted on a different image will have same kind of illumination pattern. This creates a problem as the image under consideration though being fabricated image generated using spliced objects from a same source is treated as genuine. This leads to a false positive that the image is genuine even though it is manipulated.
  As can be seen in Fig. 7, objects C and D are spliced from same source image A into the image B and have the same illumination direction estimation. The image B on checking for forgery is detected as genuine image as both the objects C and D exhibit the same illumination pattern but actually this is a case of image forgery. Hence, checking of illumination direction of objects present in the image is insufficient and an enhancement in the technique is expected.

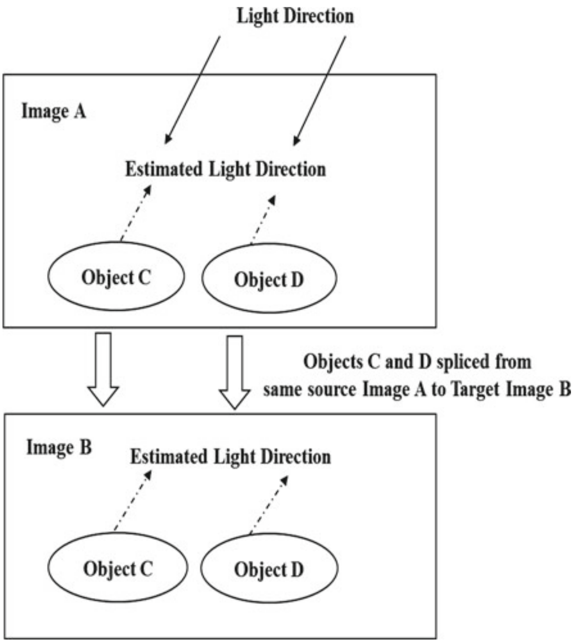

Light Direction
Image A
Estimated Light Direction
Object C
Object D
Objects C and D spliced from same source Image A to Target Image B
Image B
Estimated Light Direction
Object C
Object D

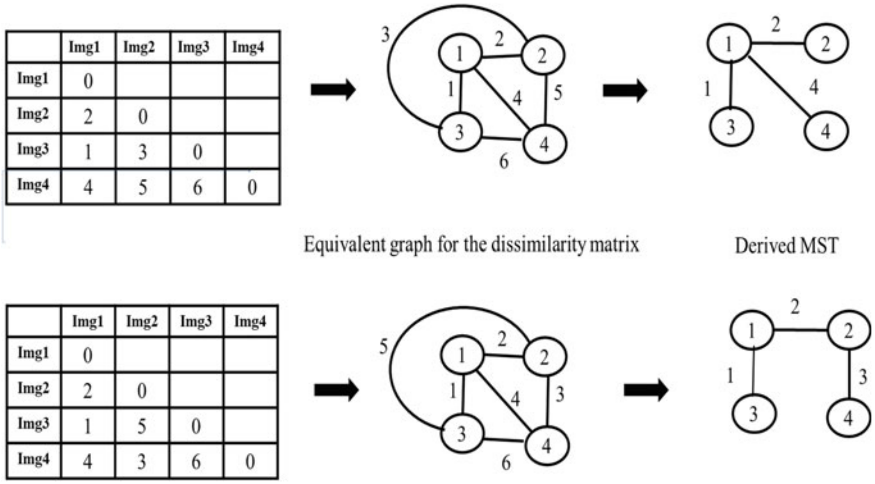
Fig. 7 Incorrect illumination direction estimation due to spliced objects from same source

4.2 Image Forgery Detection and Source Camera Identification

In this case, a hash comprising of both device features and image features is generated. There are techniques proposed for detection of forgery and source device. However, there is a need to distinguish between genuine perceptually robust image manipulation operation like rotation and scaling with those of forgery image manipulation operation while examining source camera. On combining approaches related to detection of source camera and image forgery, there is an increase in false alarms where genuine image editing operations are detected as manipulation [22]. There are techniques that can attain perceptual robustness of around 99% working independent of source device identification. Incorporating them with those of source device identification and manipulation detection is required. As currently employed techniques that can detect image forgery and distinguish between perceptual robust operation too are only around 90% which can be further tried for improvement.

4.3 Image Provenance Analysis for Tracking Image History

Provenance graph gives a set of all images related to a given query image and possible derivation tree for that image. The donor images could be of varied sizes and can



	Img1	Img2	Img3	Img4
Img1	0			
Img2	2	0		
Img3	1	3	0	
Img4	4	5	6	0

Equivalent graph for the dissimilarity matrix

Derived MST

	Img1	Img2	Img3	Img4
Img1	0			
Img2	2	0		
Img3	1	5	0	
Img4	4	3	6	0

Fig. 8 Effect of near-duplicate images on conversion of dissimilarity matrix to provenance graph

represent multiple regions in the given query image. Identifying the related images from a huge database of images is a challenging task as the amount of comparisons increase. Following are the challenges associated to the study in this domain:

- Small donor identification in provenance analysis for image forgery detection: When the contributing donors for a query image become small in size accounting for size as less as 1 to 10% of total image size it becomes difficult tracing its features and matching them with related images from the database. The recall rate for donors of small sizes is approximately in the range 55–58% [23]. In comparison to donors of medium and large size that have recall rate of small donor between 75 and 80% the recall rate of small donors needs to be improved. Hence, a check on appropriate analysis of small donors is important in the process of provenance analysis.
- Improving the dissimilarity matrix construction by considering noise from near-duplicate images:
  Provenance graph is generated using the minimum spanning tree algorithm computed over the dissimilarity matrix. If there is a minor change in the values of the dissimilarity matrix due to noise from near-duplicate images it would change the entire derivation process of graph as the spanning tree would vary. It is thereby important to extract features of the images that are near duplicates with care in order to distinguish them properly and derive appropriate graph. Figure 8 shows the actual distance between images Img1, Img2, Img3 and Img4 and a slightly modified dissimilarity matrix due to noise from the near-duplicate images. An equivalent graph for the stated matrix and the spanning tree is also stated for both original and modified dissimilarity matrices. The images Img2, Img3 and Img4 are all derived from Img1. A slight modification in the matrix changes the entire

derivation process of the images. As can be seen that Img1 is the prominent root Image from which Img2 and Img3 are derived same as previous tree. However, Img4 is derived from Img2 which is different from the previous case of original tree. Hence, a small change in the values of dissimilarity matrix can change the entire provenance graph constructed. This signifies the importance of dealing with near-duplicate images efficiently.

- Provenance graph construction using features other than image properties: Graphs constructed relying on only image features lose on certain important features which can help build provenance graph quickly. Using metadata present in images rather than merely image features can be useful in reducing the time associated for the entire provenance analysis.

5 Research Direction

Possible area of research for the stated research gaps in the discussion section is mentioned below:

- Passive image forgery detection using illumination-based techniques: Analysis of images using passive forgery detection mechanism requires detection and estimation of illumination direction of various objects present in the image. This illumination direction estimation can be erroneous if objects cast shadow over each other. This leads to the problem of concluding that an image is forged despite being genuine and raising false alarms. Also, an image generated using components from same donors will be estimated to have same illumination direction. Hence, checking merely the illumination direction of objects in the image will be insufficient. Checking of background illumination could be a possible alternative.
- Image Forgery Detection using Source Camera Identification: Techniques for image forgery detection using source camera identification are based on detection of features from images and camera or capturing device. The features extracted from this technique should be able to well distinguish between operations that are genuine and those that have manipulated the image content. Some of the operations that are performed over images to improve their quality are rotation and scaling. If operations that are genuine are identified as forgery it will lead to unnecessary false alarms. Hence, there is a need to check the nature of manipulation while checking for the source of forgery. A technique suitable in both the cases needs to be devised.
- Improving Image Provenance Analysis Process: Provenance graphs constructed using the phases of image filtering and provenance graph construction require searching huge database of images and deducing relationship between images. This process gets difficult as the search space is very large and there could be multiple objects of varied sizes in the query image. Small donors affect the accuracy of the approaches used as slight modifications like converting digit 0–8 or 1–7 in an

image is not easy to identify. Hence, there is a need to improvise provenance graph construction for small-sized donors.

The search and comparison phases in case of provenance graph construction are very large. Image metadata provide useful information like date, compression strategy, etc. which can be helpful in the provenance graph construction [12]. Rather than merely relying on the image features other complimentary aspects that come with an image need to be analysed, which may help speed up the process of provenance graph generation.

Provenance graph is built using minimum spanning tree algorithm from the dissimilarity matrix. If there is variation in the dissimilarity matrix the provenance graph will too vary. The chances of variation increase when the images are near duplicate of each other. Hence, near-duplicate images need to analysed before building the provenance graph.

6 Conclusion

A detailed review on passive method of detecting forgery through illumination detection is discussed in the paper. Areas where both image properties and capturing device properties are given attention to check for information contributing in detection of forged images is also a topic of discussion in this paper. A discussion regarding provenance analysis for building derivation tree for entire image manipulation process is mentioned in detail. Research direction and areas to explore in the field on digital image forensics are elaborated well in the paper.

7 Future Scope

In future, the problem of image forgery detection can be used to address issues like considering societal impact on a particular forgery. This cultural trend will help understand the reason for a particular manipulation better. Detection of video manipulation which is also a mode of multimedia information transfer can turn deceptive if modification of sequence of images present in the video is carried out. These further areas of research can be fruitful broad domains of study.

References

1. Cao Y, Zhang L, Chang C (2016) Using image sensor PUF as root of trust for birthmarking of perceptual image hash. In: 2016 IEEE Asian hardware-oriented security and trust (AsianHOST)
2. Zheng Y, Dhabu S, Chang C (2018) Securing IoT monitoring device using PUF and physical layer authentication. In: 2018 IEEE international symposium on circuits and systems (ISCAS)

3. Zheng Y, Cao Y, Chang C (2020) A PUF-based data-device hash for tampered image detection and source camera identification. IEEE Trans Inf Forensics Secur 15:620–634
4. Davarzani R, Mozaffari S, Yaghmaie K (2016) Perceptual image hashing using center-symmetric local binary patterns. Multimed Tools Appl 75:4639–4667
5. Roy A, Chakraborty R, Sameer U, Naskar R (2017) Camera source identification using discrete cosine transform residue features and ensemble classifier. In: *2017 IEEE conference on computer vision and pattern recognition workshops (CVPRW)*
6. Sameer V, Sarkar A, Naskar R (2017) Source camera identification model: Classifier learning, role of learning curves and their interpretation. In: *2017 international conference on wireless communications, signal processing and networking (WiSPNET)*
7. Teerakanok S, Uehara T (2019) Copy-move forgery detection: a state-of-the-art technical review and analysis. IEEE Access 7:40550–40568
8. Matern F, Riess C, Stamminger M (2020) Gradient-based illumination description for image forgery detection. IEEE Trans Inf Forensics Secur 15:1303–1317
9. Moreira D, Bharati A, Brogan J, Pinto A, Parowski M, Bowyer K, Flynn P, Rocha A, Scheirer W (2018) Image provenance analysis at scale. IEEE Trans Image Process 27:6109–6123
10. Pinto A, Moreira D, Bharati A, Brogan J, Bowyer K, Flynn P, Scheirer W, Rocha A (2017) Provenance filtering for multimedia phylogeny. In: 2017 IEEE international conference on image processing (ICIP)
11. Bharati A, Moreira D, Pinto A, Brogan J, Bowyer K, Flynn P, Scheirer W, Rocha A (2017) U-Phylogeny: undirected provenance graph construction in the wild. In: *2017 IEEE international conference on image processing (ICIP)*
12. Shichkina Y, Tishchenko V, Fatkieva R (2020) Synthesis of the method of operative image analysis based on metadata and methods of searching for embedded images. In: *2020 9th mediterranean conference on embedded computing (MECO)*
13. Bharati A, Moreira D, Brogan J, Hale P, Bowyer K, Flynn P, Rocha A, Scheirer W (2019) Beyond pixels: image provenance analysis leveraging metadata. In: 2019 IEEE winter conference on applications of computer vision (WACV)
14. Bharati A, Moreira D, Flynn P, Rezende Rocha A, Bowyer K, Scheirer W (2021) Transformation-aware embeddings for image provenance. IEEE Trans Inf Forensics Secur 16:2493–2507
15. Fernandez J, Pandian N (2018) JPEG metadata: a complete study. In: 2018 international conference on recent trends in advance computing (ICRTAC)
16. McKeown S, Russell G, Leimich P (2017) Fast filtering of known PNG files using early file features
17. Gloe T (2012) Forensic analysis of ordered data structures on the example of JPEG files. In: 2012 IEEE international workshop on information forensics and security (WIFS)
18. Mullan P, Riess C, Freiling F (2019) Forensic source identification using JPEG image headers: the case of smartphones. Digit Investig 28:S68–S76
19. Rhee K (2020) Detection of spliced image forensics using texture analysis of median filter residual. IEEE Access 8:103374–103384
20. Sekhar P, Shankar T (2021) Splicing forgery localisation using colour illumination inconsistencies. Int J Electron Secur Digit Forensics 13:346
21. Kumar S, Kasiselvanathan, Vimal (2021) Image splice detection based on illumination inconsistency principle and machine learning algorithms for forensic applications. In: 2021 smart technologies, communication and robotics (STCR)
22. Tang Z, Zhang X, Li X, Zhang S (2016) Robust image hashing with ring partition and invariant vector distance. IEEE Trans Inf Forensics Secur 11:200–214
23. Zhang X, Sun Z, Karaman S, Chang S (2020) Discovering image manipulation history by pairwise relation and forensics tools. IEEE J Sel Top Signal Process 14:1012–1023
24. Castelletto R, Milani S, Bestagini P (2020) Phylogenetic minimum spanning tree reconstruction using autoencoders. In: ICASSP 2020 IEEE international conference on acoustics, speech and signal processing (ICASSP)

25. Thakur R, Rohilla R (2020) Recent advances in digital image manipulation detection techniques: a brief review. Forensic Sci Int 312:110311
26. Yao H, Xu M, Qiao T, Wu Y, Zheng N (2020) Image forgery detection and localization via a reliability fusion map. Sensors (Basel) 20:6668
27. Kadam K, Ahirrao S, Kotecha K (2022) Efficient approach towards detection and identification of copy move and image splicing forgeries using Mask R-CNN with MobileNet V1. Comput Intell Neurosci 2022:6845326
28. Tolias G, Jégou H (2014) Visual query expansion with or without geometry: refining local descriptors by feature aggregation. Pattern Recognit 47:3466–3476