Image Forensic Tool (IFT):
Image Retrieval, Tampering Detection, and Classification

Digambar Pawar, University of Hyderabad, India
Mayank Gajpal, University of Hyderabad, India

ABSTRACT

Images are often used as an authenticated proof for any cyber-crime. Images that do not remain genuine can mislead the court of law. The fast and dynamically growing technology doubts the trust in the integrity of images. Tampering mostly refers to adding or removing important features from an image without leaving any obvious trace. In earlier days, digital signatures were used to preserve the integrity, but various tools are now available to tamper with digital signatures as well. Even in various state-of-the-art works in tamper detection, there are various restrictions in the type of inputs and the type of tampering detection. In this paper, the researchers propose a prototype model in the form of a tool that will retrieve all the image files from given digital evidence and detect tampering in the images. For various types of tampering, different tampering detection algorithms have been used. The proposed prototype will detect if tampering has been done or not and will classify the image files into groups based on the type of tampering.

KEYWORDS

Cyber-Crime, Digital Forensics, Image Forensics, Image Tampering, Tampering Classification, Tampering Detection

INTRODUCTION

In today's digital world image files play a crucial role. One of the basic forms of information available is in the form of images as it can be easily interpreted by humans. In no time, this kind of information can be shared to various people in different parts of the world. Therefore the integrity of such information is very important. An image file can be easily tampered using various techniques discussed in the later part of this paper. A tampered image can be harmful in various sensitive cases and its range can't be imagined (Farid, 2006). On the other hand, tampering of any image is much easier than identifying the tampering done. Hence, tamper detection is one of the most required fields to look into in today's scenario of digital forensics. The only way to detect whether tampering has been performed or not in a digital forensic process is by using image processing techniques (Katzenbeisser, 1999). A proper forensics process is required for verification of such image files (Böhme, 2009). In this paper, the authors have designed a prototype for performing image forensics and implemented the same for the usage of law enforcement. Image forensics is unavoidable in many cases. Modification or tampering of images that are further used for ill-intentions are increasing day by day. Recent such examples (Redi, 2011, p.2) can be seen in Figures 1 and 2.

DOI: 10.4018/IJDCF.287606

Figure 1. The tampered image of Jeffrey Wong Su En while receiving the award from Queen Elizabeth II (W Taktak, 2011)

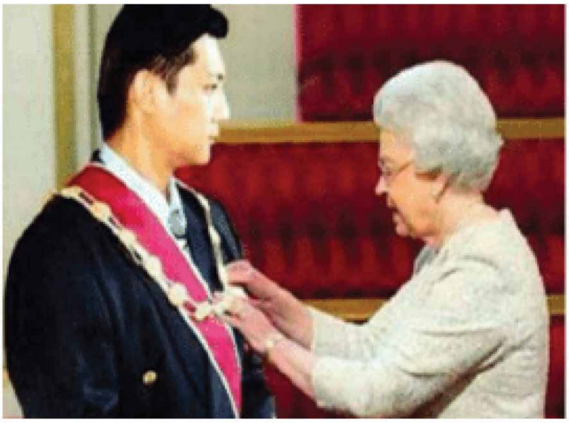
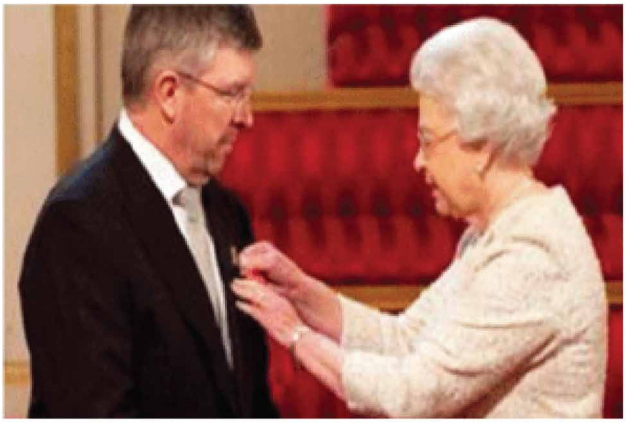


Figure 2. The original image of Ross Brawn receiving the order of the British Empire from the Queen (W Taktak, 2011)



Another important example with a different view of image tampering can be seen in Figures 3 and 4.

One can easily imagine the importance of image forensics in this case as it is related to a crime scene and the tampered image can mislead the cybercrime investigation. In this case, the detection algorithm will have to check the authenticity of the image as well as the area of the tampering. In the present day scenario, editing any given image is no longer an art of an expert; it can be performed by anyone. Hence, day to day increase in the various types of editing tools make things really hard for tamper detection. Even today with much advancement of technology, the researchers are lacking an automated image forensic tool that can easily detect tampered images with more accuracy. In this direction, the paper aims to build a robust and reliable Image forensic Tool for image tampering detection and classification. The major contributions of the paper can be summarized as:

- Retrieval of various image files from a hard disk image.
- Detection of tampering in various image file formats.
- Classification of images based on type of tampering performed.

Figure 3. Original image of a crime scene (B Soni, 2018)

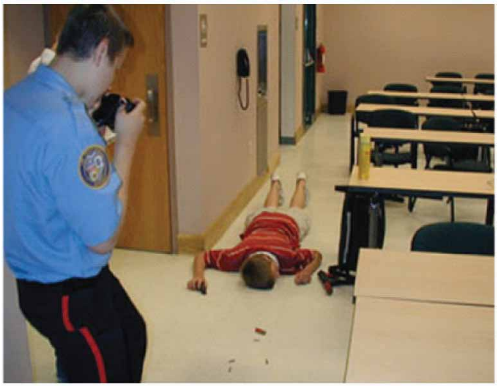
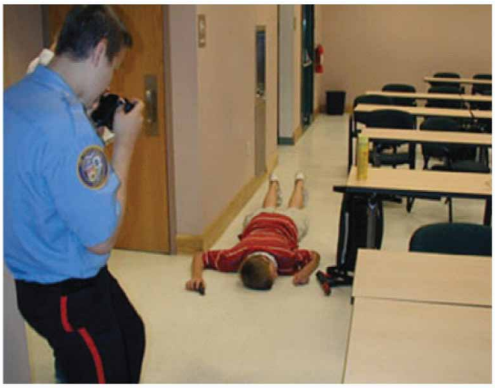


Figure 4. Tampered image in which evidence is altered (B Soni, 2018)



The rest of the paper is organized as follows. Section 2 provides the background of the proposed work. Section 3 presents a review of recent studies in the area of proposed research. In section 4, the authors present the methods of image files retrieval (from forensic disk image), various types of tampering detection and classification. Also, this section provides the complete details of the implementation with results. Conclusion and future work are provided in the sections 5.

BACKGROUND

Digital Image tampering detection techniques can be broadly classified into two types such as active detection techniques and passive (blind) detection techniques (Mishra, 2013, p.4). In active detection technique, the researchers have prior information about the image. Methods used in active detections can be watermarking and digital signature. In passive detection technique, no such information about the image is present within the image or somewhere else. The well-known researched techniques available in the literature for passive tamper detection are copy-move detection and splicing detection (Mishra, 2013). In Table 1, the complete details of image tampering techniques with detection algorithms are provided.

Table 1. Details of image tampering techniques

S. No	Technique	Algorithm	Pros	Cons
1	Watermarking	Embedding Watermark in Digital Image (Rey, 2002)	1) Easy to detect with less complexity.	1) Decreases the quality of image. 2) Accuracy is very low.
2	Digital Signature	Self-generated Verification Code(Digital Signature) during image acquisition (Mani, 2018)	1) It is embedded inside the image, hence does not affect the quality of image.	1) Can be easily tampered and hence is not trustworthy. 2) Computation complexity can increase
3	Copy-move detection	Block-based Copy Move Forgery Detection (Soni, 2018)	1) Detects tampering much accurately	1) Time complexity is high 2)Not invariant to scaling and rotation
		Key points based Copy Move Forgery Detection (Kaur, 2015)	1) Very fast in computation	1) Accuracy depends upon the key points extracted. if key points are inaccurate, accuracy will decrease.
4	Splicing	Detect image splicing with artificial blurred boundary (Liua, 2013)	1) Detects splicing accurately, even those which can't be recognized by naked eyes.	1) It is mandatory that blurring of boundaries should be done after splicing; otherwise the algorithm fails to detect it.
		Detecting JPEG image forgery based on double compression (Junwen, 2009)	1) Does not depend upon the type of editing performed 2) Detects all types of splicing performed	1) It is limited to only the JPEG file format. Does not work with other formats.
5	Retouching	Demography-based Facial Retouching Detection using Subclass Supervised Sparse Auto Encoder (Bharati, 2017)	1) Robust to the type of input given. 2) Classifies tampered images accurately.	1) Cannot identify the area of tampering

THE LITERATURE REVIEW

Image tampering has a vast history. First image tampering can be dated back to the 1800s. Since then various researchers have come up with many different approaches. One of the common approaches was using the statistical property of image (Lu, 2008). One more approach of tampering detection can be using noise features of an image (Gou, 2007). Apart from these, various machine learning classifiers are also built to determine the integrity of an image (Lyu, 2005). Approach that is specific to the type of tampering performed is block based approach which is a well-known method for copy-move forgery detection (Huang, 2011). One more thought-provoking approach is using "Energy Deviation Measure". Energy Deviation Measure is proposed as a measure of energy deviation in pixel neighborhoods in tampered and recompressed images (Gupta, 2018). Using camera parameters was also one of the approaches (Fernández, 2018), but due to the increase in the number of different types of cameras this approach is not recommended and accepted.

As the world moves towards Artificial Intelligence, various deep learning approaches have emerged in recent years (Bharati, 2016, p.6). With deep learning concepts various models have been developed for different purposes (for example object detection), such models can also be used for tampering detection. As models for specific tampering detection are not available yet, better accuracy can still be expected from deep learning concepts (Roy, 2020). Some of the latest work in the field of image tamper detection can be seen by the use of Artificial Intelligence. PRNU-based detection of facial retouching (C. Rathgeb, 2020) is one of its kinds. Apart from this, blobs and BRISK features of an image are also used in some of the latest work to detect copy move forgery (Patrick Niyishaka, 2020). Using another machine learning approach, proposing a differential retouching detection system (N. E. Haryanto, 2020) can also be seen.

A prominent way of detecting splicing forgery is using JPEG compression properties. Fridrich et al. (Fridrich, 2015), proposed a low-complexity Discrete Cosine Transform Residual (DCTR) feature utilizing first order statistics of quantization noise residual obtained from the decompressed JPEG image using 64 kernels of the discrete cosine transform of JPEG image. Recent work of splicing detection for color images based on quaternion discrete cosine transform (Jinwei Wang, 2020) was also proposed. Some more recent work in detecting splicing forgery has been based on the local descriptor of an image (Yuan Rao, 2020). Using deep learning local descriptor, splicing detection and localization is achieved. For copy-move forgery detection, Popescu and Farid (Popescu, 2004) developed a method based on Principal Component Analysis (PCA). This method does not stand good for lossy compression because of the dimensionality reduction feature of PCA. One effective method of copy-move forgery detection is based on block-based techniques. Zhang et al. (Zhang, 2008, p. 4) applied Discrete Wavelet Transform (DWT) on a forged image by decomposing it into four frequency sub-bands, and further divided the approximate sub-band into overlapping blocks. Another effective and more accurate method is using the Key point feature. David G. Lowe (Lowe, 1999) came up with the idea of key point for object detection but can be alternatively used for copy-move forgery detection. In some recent works fractional quaternion zernike moments were proposed to detect color image copy move forgery (Beijing Chen, 2018). For retouching detection, most of the work has been done from the point of view of Machine learning or deep learning.

From various techniques proposed by eminent researchers in this field, authors have considered a few best algorithms which will be more appropriate to their requirements suitably with the best time complexity. Taking these algorithms as a basis, the authors have devised an algorithm that can take any type of image file as input and provide the output irrespective of the type of tampering is performed.

IMAGE FORENSIC TOOL

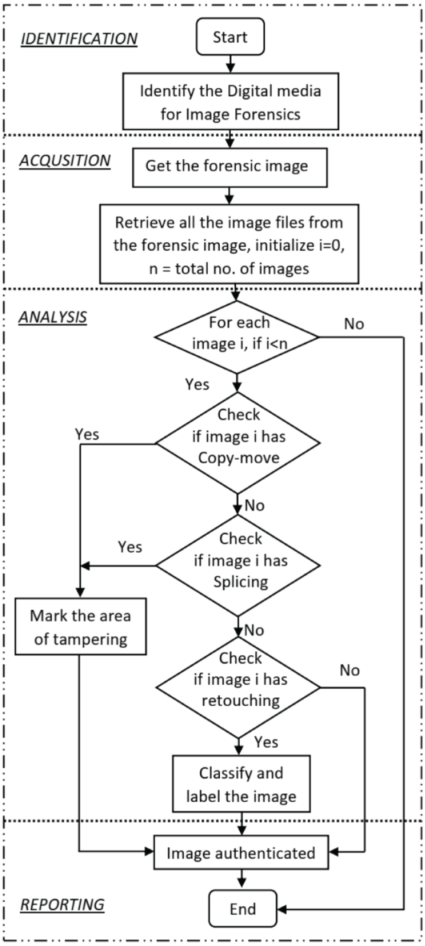
One of the early definitions of digital forensics was provided by McKemmish in 1999 as "*The process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable by court of law*" (McKemmish, 1999). In the similar lines, image forensics can be defined as "*The process of identifying, acquiring, analyzing and reporting digital evidence related to images in a manner that is legally acceptable by court of law*". The control flow diagram of the proposed "Image forensic Tool" as shown in Figure 5, is fundamentally a way forward to achieve the goal of this definition. The flow of control of the proposed model is self-explanatory and enables the forensic investigators to perform analysis related to image forensics. The model is divided into four phases. In the phase of identification, the digital device which has to be investigated will be identified. For forensics purposes, its forensic image (bit-by-bit copy of the digital device) is made in the acquisition phase.

This can be performed using hardware tools (Tableau forensic duplicator, HardCopy 3P, etc.) or software tools (FTK imager, EnCase Forensic Imager, TrueBack, etc.) (Povar, 2015, p. 49). From the acquired forensic image, the authors need to get all the picture files (.jpg, .png, .bmp, etc.) using the technique called file carving (Povar, 2011). File carving is a process of recovering files based on the analysis of file formats (usually metadata of the files like header, footer, and file size). Once all the picture files are retrieved, image tampering detection is performed in the analysis phase. Finally, the process ends with the authentication (originality check) of the picture files in the reporting phase.

Copy-Move Forgery Detection Technique

Copy-move forgery involves copying a portion of an image and pasting it on to a different location in the same image. To achieve copy-move forgery various image-editors are available in which a portion can be copied and pasted in the same image. For better results, a Key point based method

Figure 5. Control flow diagram of Image Forensic Tool


IDENTIFICATION
Start
Identify the Digital media for Image Forensics
ACQUSITION
Get the forensic image
Retrieve all the image files from the forensic image, initialize i=0, n = total no. of images
ANALYSIS
For each image i, if i<n
No
Yes
Check if image i has Copy-move
Yes
No
Check if image i has Splicing
Yes
Mark the area of tampering
No
Check if image i has retouching
No
Yes
Classify and label the image
Image authenticated
REPORTING
End

in combination with SWT (Stationary Wavelet Transform) has been used. Previous key point based algorithms without SWT gives less accurate results(M Mishra, 2013). Other block based methods are also less accurate than key point based methods with SWT(B soni, 2018).

Steps involved in Copy-move forgery detection technique are:

Step 1: Image is converted into grayscale.
Step 2: SWT is applied to decompose the image into 4 components:
a. Approximate component
b. Horizontal component
c. Vertical component
d. Diagonal component
Step 3: Approximate component of SWT is used as an input parameter for the SIFT algorithm.
Step 4: SIFT accurately detects the key points and descriptor.
Step 5: Matching key points are detected using Euclidean distance which crosses a threshold value (0.55).
Step 6: Lines are drawn between matched key points to display tampered areas.

If the image file shown in Figure 6 is considered as input to the above algorithm, the outcome of the algorithm is shown in Figure 7.

Figure 6. Tampered image using Copy-move forgery (B Wen, 2016, p.1)

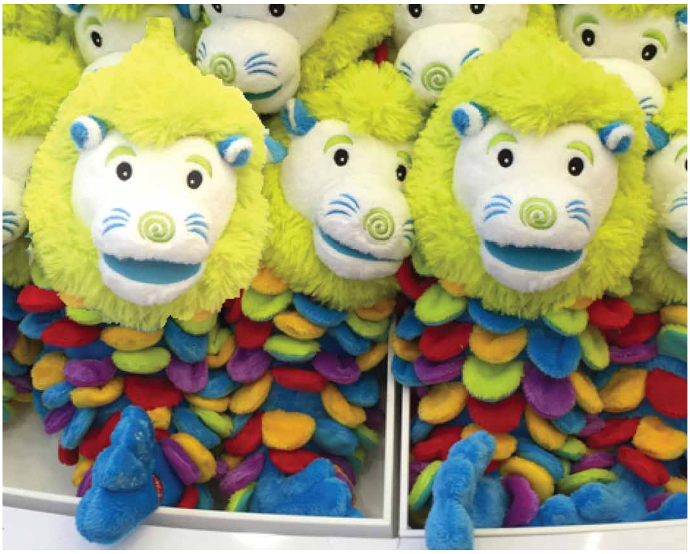


Figure 7. Marked area of tampering

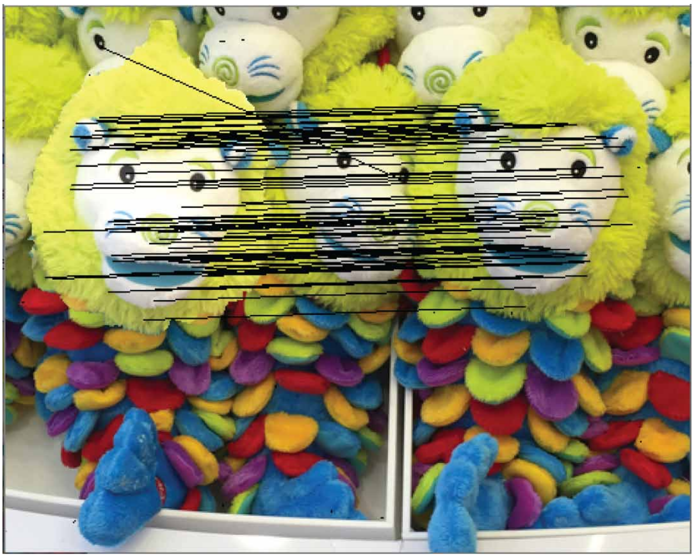
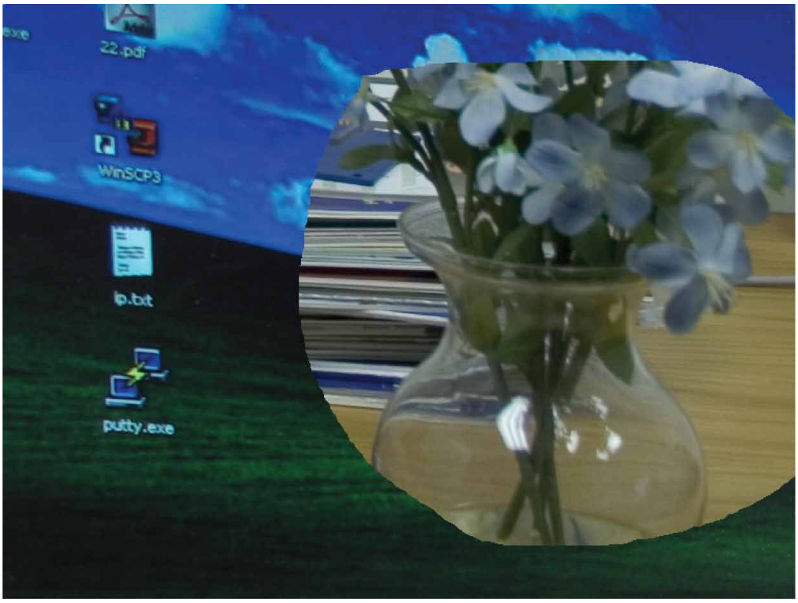


Figure 8. Tampered image (Splicing forgery) (Y Hsu, 2006)



Splicing Detection Technique

Splicing forgery is defined as copying a portion of an image to any location of another image. When a portion of an image is copied and pasted to another image, it changes the characteristics of the tampered image. Detecting spliced images will be challenging as differentiating pixels from alien images and pixels from original images is difficult. In the proposed technique, the authors have considered image edges rather than pixels. Usually there are sudden changes in edges of spliced areas of an image. There are various other methods of detecting splicing that includes artificial blurred boundary (G Liua, 2013), double compression (W Junwen, 2013). Comparison of those methods with the proposed method is mentioned in the results section.

Steps involved in Splicing forgery detection technique are:

Step 1: For each color channel i.e., R,G,B, detect abrupt change with order filtering in horizontal and vertical direction.
Step 2: Horizontal denoise: OSF(img,2,1*3).
Step 3: Horizontal derivation: Used sobel in y-direction(x-direction for vertical), output be D.
Step 4: Calculate absolute difference: AB=abs[D-OSF(D,3,1*5)].
Step 5: Combine all color channels and horizontal normalized sharpness is obtained by:

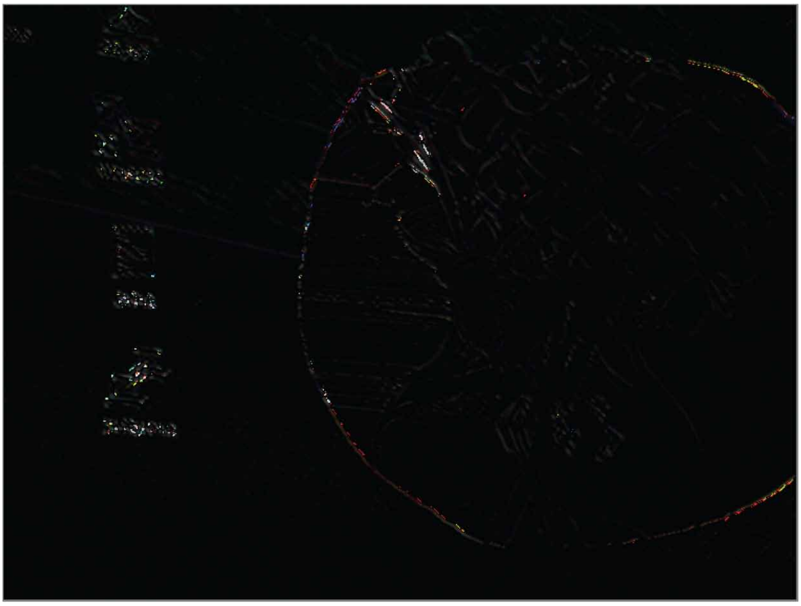
HN=AB/AB+OSF(AB,2,1*5)

Step 6: Combine Horizontal and vertical directions, HV=max(HN,VN) and obtain a final normalized sharpness:

NS=HV/HV+OSF(HV,10,5*5)

The result of the above algorithm with the input image as shown in Figure 8 is provided in Figure 9.

Figure 9. Highlighted edges of tampered area



Retouching Detection Technique

Retouching is the polishing of an image. Retouching is the process of altering an image to prepare it for final presentation. Retouching commonly involves adjustment of colors, brightness, contrast etc. A number of applications are available to perform retouching in an image. Retouching can vary from increasing brightness of an image to totally changing any face in an image. In the proposed model, ELA (Error Level Analysis) has been used for detecting retouching forgery. For classification, Random Forest model is being used. Steps involved in Retouching forgery detection technique are:

Step 1: Take an image of any format and convert it into jpeg format.
Step 2: Write a temporary image with a lower quality level than the original image.
Step 3: Take the difference of the temporary image and original and save the file, the file obtained is the ELA image of the original.
Step 4: The ELA image will be given as an input to the Random Forest model, which is already trained.
Step 5: Successful testing of an image by Random Forest model will be able to label the image as tampered or original.

The image file that is shown in Figure 10 is classified as a tampered image as shown in Figure 11.

GUI (Graphical User Interface) of the Image Forensics Tool

The user interface of the Image Forensics tool has 3 panes (left, right and bottom). The left pane has a tree view where all image forgery categories are listed. An image which is tampered will be added to a respective category after tampering detection.

Figure 10. Tampered image (K. Asghar, 2019)

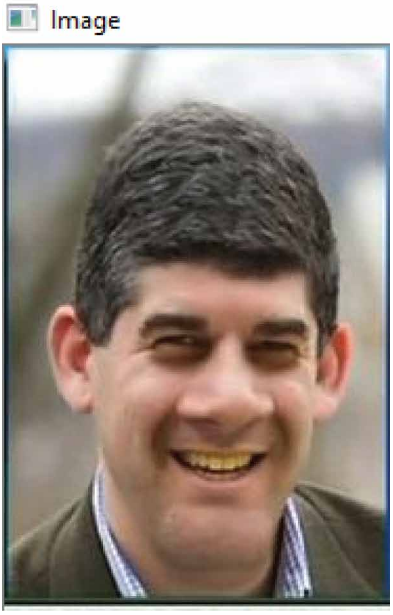
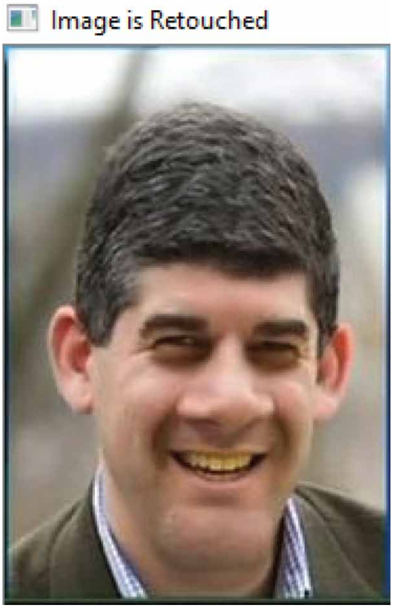


Figure 11. Classified image



On selecting a particular category in the left pane, will result in showing all the images under the category in the right pane. To view the details of an image listed under the right pane, the bottom pane is used as shown in the Figure 12.

Figure 12. Image Forensics tool

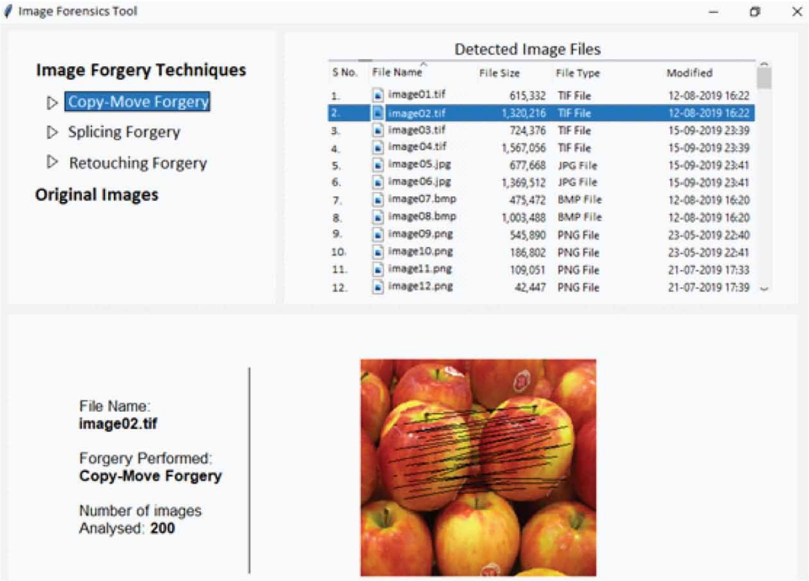


Image Forgery Techniques

- ▷ Copy-Move Forgery
- ▷ Splicing Forgery
- ▷ Retouching Forgery

Original Images

Detected Image Files

S No.	File Name	File Size	File Type	Modified
1.	image01.tif	615,332	TIF File	12-08-2019 16:22
2.	image02.tif	1,320,216	TIF File	12-08-2019 16:22
3.	image03.tif	724,376	TIF File	15-09-2019 23:39
4.	image04.tif	1,567,056	TIF File	15-09-2019 23:39
5.	image05.jpg	677,668	JPG File	15-09-2019 23:41
6.	image06.jpg	1,369,512	JPG File	15-09-2019 23:41
7.	image07.bmp	475,472	BMP File	12-08-2019 16:20
8.	image08.bmp	1,003,488	BMP File	12-08-2019 16:20
9.	image09.png	545,890	PNG File	23-05-2019 22:40
10.	image10.png	186,802	PNG File	23-05-2019 22:41
11.	image11.png	109,051	PNG File	21-07-2019 17:33
12.	image12.png	42,447	PNG File	21-07-2019 17:39

File Name:
image02.tif

Forgery Performed:
Copy-Move Forgery

Number of images
Analysed: **200**

RESULTS

Results for Copy-Move Forgery Detection

The Table 2 shows the analysis of the results of the Copy-move forgery detection method used by the proposed image forensics tool. The authors have used two different datasets for the result analysis. Coverage Dataset: This dataset contains 200 images of which 100 are original and remaining are tampered versions of the original. Coverage specifically has copy move forged images with their respective original image (B Wen, 2016, p.1). MICC F600 Dataset: This dataset is composed of 440 original images, 160 tampered images, 600 images in total (Al-qershi, 2018, p.2). This dataset is one of the oldest one available for copy move forgery. Accuracy achieved with both the datasets using the proposed model is detailed in the Table 3.

Table 2. Copy-move forgery detection results

Dataset	True Positive	True Negative	False Positive	False Negative	Accuracy
Coverage	89	87	11	13	88%
MICC F600	142	376	18	64	86.34%

With the obtained results, the authors can conclude that their modified copy move forgery detection algorithm gives a steady accuracy for different datasets. This implies that the proposed model gives a positive outcome for images originated from different sources. Few research papers which discussed these comparable algorithms do not contain the accuracy table, in such cases we have simulated their algorithm to get an approximate result.

Table 3. Comparison with existing algorithms

Dataset	Algorithm 1	Accuracy	Algorithm 2	Accuracy	Proposed	Accuracy
Coverage	Key point without SWT(M Mishra, 2013)	83.5%	Block based method(B soni, 2018)	81.5%	Key Point with SWT	88%
MICC F600	Key point without SWT(M Mishra, 2013)	82.88%	Block based method(B soni, 2018)	80.66%	Key Point with SWT	86.34%

Results for Splicing Forgery Detection

As shown in Table 4, the results analysis of Splicing forgery detection is performed using two different datasets. Columbia Dataset: This dataset contains 183 authentic images (authentic in this case means images taken from a single camera) and 180 spliced images. This dataset is dedicated for spliced images only. CASIA Dataset: CASIA contains 800 authentic images and 921 spliced images. CASIA is one of the datasets which contains a large amount of images as compared to other datasets. Performance of the proposed algorithm on these datasets is detailed in Table 5. In the authors' analysis, they have observed that Spliced forgery detection algorithm is relatively good for a dataset with a large amount of images. Hence, the proposed algorithm performed relatively superior with CASIA dataset.

Table 4. Splicing detection results

Dataset	True Positive	True Negative	False Positive	False Negative	Accuracy
Columbia Spliced Image	158	157	25	23	86.77%
CASIA Dataset	737	715	184	85	84.36%

Table 5. Comparison with existing algorithms

Dataset	Algorithm 1	Accuracy	Algorithm 2	Accuracy	Proposed Algorithm	Accuracy
Columbia Spliced Image	Blurred Boundary(G Liua, 2013)	81.37%	Double compression(W Junwen, 2009)	81.11%	Normalized sharpness	86.77%
CASIA Dataset	Blurred Boundary(G Liua, 2013)	82.88%	Double compression(W Junwen, 2009)	81.21	Normalized sharpness	84.36%

Table 6. Retouching detection results

Dataset	True Positive	True Negative	False Positive	False Negative	Accuracy
FRITH Dataset	243	148	12	7	95.36%

Results for Retouching Forgery Detection

In this case the authors have used only one dataset (FRITH Dataset) for results analysis. From the FRITH dataset, the authors have collected 255 historic images containing forgeries. Along with these, authentic versions of 155 forged images were also obtained from various sources. As shown in Table 6 and Table 7, retouching detection was done with high accuracy in comparison with previous two forgery detections. As per the authors' observation, the reason for increase in accuracy is due to the machine learning technique used in the proposed algorithm.

Table 7. Comparison with existing algorithms

Dataset	Existing Algorithm	Accuracy	Proposed Algorithm	Accuracy
FRITH Dataset	Supervised deep learning(A Bharati, 2016)	92.57%	Labeled machine learning	95.36%

CONCLUSION AND FUTURE WORK

The growth rate of child grooming is at the pace of Moore's law in recent times. The reason behind such kind of cyber-crime is the easy way of manipulating image files. In this paper, the authors have designed and developed a fully automated image forensic tool to detect tampered images. The primary focus of the proposed model is that it is independent of the type of tampering performed in the image. For any type of image, it can detect authenticity of image and type of tampering performed. In the state-of-art techniques accuracy may be high but have few limitations. The limitations can be in the form of format of an image, type of tampering performed, etc. The prototype proposed in this paper overcomes these limitations. The model that the authors have proposed uses previously implemented methods as a reference and merging them all to come up with a new prototype that can perform better for all the types of image formats. The authors have used some of the best methods to increase accuracy; for copy-move - key based method is used, for splicing - edge sharpness method is used, and finally for retouching - random forest method is used for detecting tampered images. Using such various techniques for different tampering, desired output is obtained. A limitation that the authors have observed in this proposed model is that the time taken for tampering detection and authentication is comparatively higher than the modern applications. In future, the authors would plan to improve the proposed prototype with lesser complexity and better accuracy by preserving their main objective of detecting tampered images without any particular restrictions. Hence, it could be more appropriate to come up with a prototype that uses only a single algorithm to detect all types of tampering on various image formats. Such sophisticated ways can improve image forensics to a great extent.

REFERENCES

Al-qershi, O., & Khoo, B. E. (2018). Evaluation of Copy-Move Forgery Detection: Datasets and Evaluation Metrics. *Multimedia Tools and Applications*, *77*, 31807–31833.

Asghar, K., Sun, X., Rosin, P. L., Saddique, M., Hussain, M., & Habib, Z. (2019). Edge-Texture Feature based Image Forgery Detection with Cross-Dataset Evaluation. *Machine Vision and Applications*, *30*(7-8), 1243–1262.

Bharati, A., Vatsa, M., Singh, R., & Bowyer, K. W. (2016, September). Detecting Facial Retouching Using Supervised Deep Learning. *IEEE Transactions on Information Forensics and Security*, 1903–1913.

Chen, Yu, Su, Shim, & Shi. (2018). Fractional Quaternion Zernike Moments for Robust Color Image Copy-Move Forgery Detection. *IEEE, 6,* 11277-11292.

Digambar, P. (2015). *A Novel Digital Forensic Framework for Cloud Computing Environment*. Birla Institute of Technology and Science. https://shodhganga.inflibnet.ac.in/handle/10603/125383

Digambar, P., & Bhadran, V. K. (2011). Forensic data carving, Lecture Notes of the Institute for Computer Sciences. *Social Informatics and Telecommunications Engineering*, *53*, 137–148.

Fernández, E. G., Ana, L. S. O., Luis, J. G. V., & Hernandez-Castro, J. (2018, September). Digital Image Tamper Detection Technique Based on Spectrum Analysis of CFA Artifacts. *Sensors (Basel)*, *18*(9), 2804.

Gou, Swaminathan, & Wu. (2007). Noise Features for Image Tampering Detection and Steganalysis. *ICIP 2007. IEEE International Conference on Image Processing*, 6, VI-97-VI-100.

Gupta, Mohan, & Sandhu. (2018). Energy deviation measure: a technique for digital image forensics. *Int. J. Electronic Security and Digital Forensics*, *10*(4).

Han, J. G., Park, T. H., Moon, Y. H., & Eom, I. K. (2018). Quantization-based Markov feature extraction method for image splicing detection. *Machine Vision and Applications*, *29*, 543–552.

Holub, V., & Fridrich, J. (2015). Low-complexity features for JPEG steganalysis using undecimated DCT. *IEEE Transactions on Information Forensics and Security*, *10*(2), 219–228.

Huang, Y., Wei, L., Sun, W., & Long, D. (2011). Improved dct-based detection of copy-move forgery in images. *Forensic Science International*, *206*(1), 178–184.

Jain, A., Singh, R., & Vatsa, M. (2018). On detecting GANs and retouching based synthetic alterations. *Proc. IEEE 9th Int. Conf. Biometrics Theory, Appl. Syst. (BTAS)*, 1–7.

Kaur, Saxena, & Singh. (2015, June). Key-point based copy-move forgery detection and their hybrid methods: A Review. *Journal of The International Association of Advanced Technology and Science*, *16*.

Li, J., Lu, W., Weng, J., Mao, Y., & Li, G. (2018). Double jpeg compression detection based on block statistics. *Multimedia Tools and Applications*, 3452–3468.

Liua, , Wang, Lianc, & Dai. (2013). Detect image splicing with artificial blurred boundary. *Mathematical and Computer Modelling*, *57*, 2647–2659.

Liua, , Wang, Lianc, & Dai. (2013). Detect image splicing with artificial blurred boundary. *Mathematical and Computer Modelling*, *57*, 2647–2659.

Lowe, D. G. (1999, September). Object Recognition from Local Scale-Invariant Features. *Proc. of the International Conference on Computer Vision*.

Lyu, S., & Farid, H. (2005). How realistic is photorealistic? *IEEE Transactions on Signal Processing*, *53*(2), 845–850.

Mishra & Adhikary. (2013, JUNE). Digital Image Tamper Detection Techniques - A Comprehensive Study. *International Journal of Computer Science and Business Informatics, 2*(1).

Niyishaka, P., & Bhagvati, C. (2020). Copy-move forgery detection using image blobs and BRISK feature. *Multimedia Tools and Applications*, *79*(35-36), 26045–26059. doi:10.1007/s11042-020-09225-6

Raja Mani, P., & Lalitha Bhaskari, D. (2018). Image Tamper Detection and Localization based on self-generated Verification Code during Image Acquisition. *International Journal of Applied Engineering Research, 13*, 2110-2118.

Rao, Y., Ni, J., & Zhao, A. H. (2020). Deep Learning Local Descriptor for Image Splicing Detection and Localization. *IEEE Access: Practical Innovations, Open Solutions*, *8*, 2970735–2970751.

Rathgeb, Satnoianu, Haryanto, Bernardo, & Busch. (2020). Differential Detection of Facial Retouching: A Multi-Biometric Approach. IEEE, 8, 2020, 24312-24326.

Rathgeb, C., Botaljov, A., Stockhardt, F., Isadskiy, S., Debiasi, L., Uhl, A., & Busch, C. (2020). PRNU-based Detection of Facial Retouching. IET Biometrics Journal.

Rathgeb, C., Dantcheva, A., & Busch, C. (2019). Impact and detection of facial beautification in face recognition: An overview. *IEEE Access: Practical Innovations, Open Solutions*, *7*, 152667–152678.

Redi, J. A., Taktak, W., & Dugelay, J.-L. (2011). Digital image forensics: A booklet for beginners. *Multimedia Tools and Applications*, *51*(1), 133–162. doi:10.1007/s11042-010-0620-1

Rey, C., & Dugelay, J.-L. (2002). A survey of watermarking algorithms for image authentication. *EURASIP JASP*, *6*(6), 613–621. doi:10.1155/S1110865702204047

Roy, Dixit, Naskar, & Chakraborty. (2020). Digital Image Forensics Theory and Implementation. *Studies in Computational Intelligence, 755.*

Soni, B., & Biswas, D. (2018). Image Forensic using Block-based Copy-move Forgery Detection. *5th International Conference on Signal Processing and Integrated Networks (SPIN).*

Wang, , & Liu, , & Dai. (2009). Detecting JPEG image forgery based on double compression. *Journal of Systems Engineering and Electronics*, *20*(5), 1096–1103.

Wang, J., Liu, R., Wang, H., Wu, B., & Shi, Y.-Q. (2020). Quaternion Markov Splicing Detection for Color Images Based on Quaternion Discrete Cosine Transform. *Transactions on Internet and Information Systems (Seoul)*, *14*, 2981–2997.

Wen, B., Zhu, Y., Subramanian, R., Ng, T., Shen, X., & Winkler, S. (2016). COVERAGE – A Novel Database for Copy-move Forgery Detection. *Proc. IEEE Int. Conf. Image Processing (ICIP).*

Zhang, J., Feng, Z., & Su, Y. (2008). A new approach for detecting copy-move forgery in digital images. *11th IEEE Singapore International Conference on Communication Systems, ICCS*, 362–366.

Dr. D. Pawar is currently Associate Professor at the School of Computer and Information Sciences, University of Hyderabad, India. He worked as a faculty in the Dept. of Computer Science and Information Systems at BITS Pilani, Hyderabad Campus. He was associated as Scientist with the Centre for Development of Advanced Computing (CDAC), Trivandrum, India. He was instrumental in design and development of computer forensic analysis tools at CDAC. His research areas include Computer Forensics, Cloud Computing, IoT, Fog Computing, and Information Security.