Fake Image Identification using Image Forensic Techniques

Satyendra Singh, Rajesh Kumar
Departments of Electronics & Communication, JK Institute of Applied Physics and Technology, University of Allahabad, Prayagraj, UP, India

Keywords: Image forensic, Photo Forgery Detection, Copy-move Image Forgery, Splicing

Abstract: These days' digital images are a popular way of information sharing. it is known that the uses of images have diverse areas such as news, magazine, medical, education and entertainment etc. this popularity of digital images creates an opportunity for the researchers to ensure trustworthiness of an images. Due to all these important utilities, the digital image has been successfully making it place in society. In this era of digitalization image editing software is available in cheap mobile devices. That can generate fake image easily. Fake images have been used by some organisations for influencing election, and violence and rumour in the society. This paper focus on forgery detection techniques of fake images and understand the usability of proposed technique for better accuracy of fake image detection.

1 INTRODUCTION

Digital image is a collection of picture elements(pixel), digital images used in various areas such as social media, news courtrooms, entertainment, political campaigns and so on. The use of digital image is growing very fast today, digital image has become an important means of sharing information, even in a small meeting or an important event, we all use digital cameras or camera enabled mobile devices. Capture every social media. But with the speed of digital images are becoming popular among us, the trend of fake image is also increasing. It is difficult to ensure the integrity and authenticity of the image due to tempering of the images.

Nowadays image manipulation application software is easily available on cheap mobile devices. And by using some powerful software to manipulate image, without leaving obvious visual clues. Image authenticity problems occur in application that is courtroom, mass media and so on. Concerning authenticity problems of digital images. Therefore, image an important issue in forensic science.

The digital image manipulation is widely used in bad aim and hiding original information of an image has a long history. The history of photo forgery is very long. Photo has been used by people for a long time, but the image forgery has been used for the bad purpose. In below Figure1 shown a photo of Mao, Stalin, Hitler, Castro, Mussolini, and Brezhnev times. In this figure photograph is manipulated for better poses to erasing enemies or bottle of beer (Kim et al., 2012).

In the times of Stalin, the image manipulation is needed long hours of lengthy work in darkroom, but in the present day any one can manipulate image in few seconds by using photo editing software like adobe photoshop that cannot be easily detected. The authentication of photo tampering is necessary to secure image communication process and trustworthy of an image.

This picture was taken in the G20 summit in Hamburg, Germany. The images that are given bellow official picture of G20 summit and showing US president Trump on the side lines or lots of images showing US president and Vladimir Putin meet first time. In Figure 2 is a fake image, making the round on social media in 2017. Photo in Figure 3 is the original Getty image.

Singh, S. and Kumar, R.
Fake Image Identification using Image Forensic Techniques.
DOI: 10.5220/0010563000003161
In *Proceedings of the 3rd International Conference on Advanced Computing and Software Engineering (ICACSE 2021)*, pages 95-100
ISBN: 978-989-758-544-9

Figure 2: Fake image, making the round on social media in 2017.

Figure 3: Original Getty image

1.1 Image Forgery

Photo forgery is describe as deleting, adding, and changing few main features from digital image without leaving any sign (Qureshi et al., 2014). Image forgery is created many challenges to ensure trustworthy of an image.

Types of digital image forgery

Recent years, many ways have been employed to temper with digital images. Several types of digital photo tampering are existing.

Some common types of image forgeries are:

1. Copy-move photo tampering
2. Splicing
3. Image Morphing
4. Image Retouching.

1.1.1 Copy-Move Photo Tampering

The digital photo tampering technique is easy to implement and difficult to detect (Abidin et al., 2019). In this tampering some features of a photo are copies and pasted to another area in the same photo. In digital photo copied part can be any types (Qureshi, 2014). In figure 4 shown an example of copy move forgery.

Figure 4: Copy move forgery image.

1.1.2 Splicing

Splicing is another type of technique of image tampering. In this tempering of image forgery two or more images are used for creating tampered photo (Tembe et al., 2017). In this technique some feature of photo is copied from one photo and pasted to another photo. Image splicing is difficult to detect than copy move forgery (Majumder et al., 2018). Figure 5 shows an example of an image splicing, here left side is natural photo and right side (b) is the spliced photo.

Figure 5: Splice image.

1.1.3 Image Morphing

In morphing forgery, morphing is applied in two images. In this technique shape of photo is change to one form shape in another photo (Elaskily et al., 2017). Figure 6 an example of photo morphing photo (a) is original photo of Hillary Clinton, photo (b) is morphed photo and (c) is original photo of Donald Trump.

(A) (B) (C)

Figure 6: A is original image of Hillary Clinton, B Morphed-image and C is original photo of Donald Trump.

1.1.4 Image Retouching

This is less dangerous type of photo forgery than other types of photo forgery techniques. In this technique original photo do not changes, but some enhancement or reduces feature of original photo such as light, background and color changing to divert attention about an objective in photo. Image retouching technique is popular among smart phone-based camera users and magazine photo editors (Mankar et al., 2015). Fig.7. is an example of image retouching.

Figure 7: Retouching image.

2 LITERATURE REVIEW

(Eduard et al., 2019) present a system for detection of splicing forgery of digital image forgeries. In here method based on VGG-16 CNN. Author use CNN based method for classification of images in two parts first one is original and second forgery. And classification is used image fragments. In this paper used CASIA dataset for experiment. In this dataset images are partitioned into training and test sample in the ratio of 80:20. All the images are additionally compressed by using JPEG algorithm. Proposed CNN based algorithm used on compressed images of quality factor(Q). accuracy on Q=90 and Q=80 is 67.1% and 66.3% respectively. And in this paper, the accuracy of proposed algorithm is 97.8% for fine-tuned model and 96.4% accuracy for zero stage trained. Limitation of this algorithm, it has narrow range of accuracy. Where forge image is compressed by JPEG compression algorithm.

(Ghoneim et al., 2018) in here, author describe a system for medical photo tamper detection for smart healthcare system. Author proposed system is used for checking authenticity of an image and identify that photos related to healthcare are not change. The proposed forgery system consists of noise extraction pattern, SVM and ELM classifier and the realization of multiresolution regression filter. In this paper the proposed system is tested on three different databases, two databases CASIA 1 and CASIA 2 has original photo and other one DDSM database mammogram. The proposed method achieve accuracy 98% for original photos and 84.3% for medical photos. The method achieved best performance, when add the score of two classifiers.

(Selvaraj et al., 2020) in this study, author proposed an improved key point-based copy move forgery detection system and using a sensitivity based clustering approach. Author find that sensitivity-based clustering performs well in comparison to existing agglomerative clustering and DBSCAN algorithm. The suggested approach is also resistant to a variety of geometric attacks, such as rotation, composition and scaling.

(Dixit et al., 2020) proposed method has proved, if picture is obtained from various datasets with varied features. This method has proven to be successful in detecting forgeries. For image level and pixel level detection, the suggested approach has shown encouraging results. The proposed method shows robustness against composite attacks. Proposed approaches to detect tampered pictures that can withstand and a wider range of distortion parameters, such as non-affine transformations, in the future.

(Meena et al., 2020) author describe the Fourier Mellin Transform (FMT) and SIFT algorithm for copy move forgery detection technique. The proposed method shows very satisfactory results under various geometric transformations because the FMT and SIFT descriptors are rotation and scaling invariant in nature. Author find that the proposed technique works very good in some special condition like scaling with factor 50% - 200%, and compression in JPEG with a quality factor up to 20.

3 MATERIALS AND METHODS

There are some images and some methods to find the images are fake or not.

3.1 About Image

These images have been taken from Iranian Missile test images in the form of jpg. In figure 8 is the original image of missile test and in figure 9 is the tampered image of missile test.

Figure 8: Original image of Iranian missile test.

Figure 9: Fake image of Iranian missile test.

3.2 Methods

In the Experimental purpose Scale invariant feature transformation (SIFT) is used for copy move tamper detection. In this method some steps are applied firstly give input original or forged image converts input image data into SIFT features named sift descriptor, in second steps this feature covert into clustering SIFT then matching clustering results and finally take decision on forged or original image.

Table 1: Comparison of various tampering Detection techniques

SSN	Title	Methods	Detection Domain	Advantage
1	Tampered and computer-generated face photos identification based on deep learning (Dang et al., 2020).	Deep learning - basedframework.	Tampered and computer-generated face photos detection.	Flexible, computationally efficient, and robust against imbalanced dataset.
2	Deep learning on digital photo splicing detection using CFA artifacts (Hussien et al., 2020).	Deep learning using color filter array.	Digital image splicing.	Accuracy is 95.5%
3	Detecting fake images on social media using machine learning (AlShariah et. al.).	Deep learning technique via CNN.	Detecting fake image on social media	Accuracy is 97%
4	Copy-move tamper detection using SURF feature extraction and SVM supervised learning technique (Dhivya et al., 2020).	Speeded up robust feature (SURF) and SVM	Copy move forgery	Accuracy is 95.5%
5	Median filtering forensics in digital photos based on frequency-domain features (Liu et al., 2017).	A novel frequency domain feature	Medium filtering detection	Reduce computing and merit for mass processing data in real time.
6	Copy-move forgery detection using SIFT algorithm (Huang et al., 2008).	SIFT	Copy move forgery	This method has good performance on different types of post photo processing (such as rotation noise, scaling etc.)

4 EXPERIMENTAL RESULTS

To validate our proposed method, we performed experiment for detecting copy move forgery using scale invariant feature transformation (SIFT) algorithm. SIFT algorithm applied on copy move forged image. Following two figures are show experimental results. Figure 10 shows results of DoG pyramid images and Figure 11 result of copy move forge images.

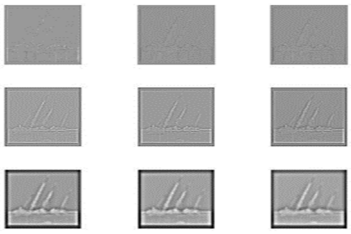

Figure 10: Results of DoG pyramid images.

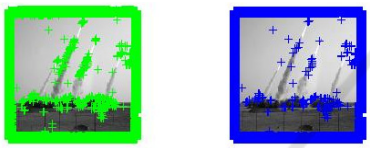

Figure 11: Result of detected feature of copy-move forged images.

For experimentation purpose MATLAB 2015a student version and window 10 operating system, 8gb RAM and processor intel core i5 has been used. In above figure green mark region using key points and blue mark region is accurate selected key points approximation. In this figure green and blue mark region show copy part of same image. SIFT is better method to detect copy move forgery.

5 CONCLUSIONS

In this work various types of digital image tampering identification techniques are studied and tested. For testing copy-move tampered image Scale invariant feature transformation algorithm has been used and experimented and experimental results show that it is better, as compared to another image forgery detection techniques. The main aim of this study is to be understanding the various image forgery detection techniques. Further this study helps to the beginners for understand fundamental steps involved in digital image forensic.

REFERENCES

Abidin, Arfa Binti Zainal, et al. (2019). "Copy-Move Image Forgery Detection Using Deep Learning Methods: A Review." 2019 6th International Conference on Research and Innovation in Information Systems (ICRIIS). IEEE.

AlShariah, N. M., Khader, A., & Saudagar, J. Detecting Fake Images on Social Media using Machine Learning.

Dixit, A., & Bag, S. (2020). Composite attacks-based copy-move image forgery detection using AKAZE and FAST with automatic contrast thresholding. IET Image Processing, 14(17), 4528-4542.

Dhivya, S., Sangeetha, J., & Sudhakar, B. (2020). Copy-move forgery detection using SURF feature extraction and SVM supervised learning technique. *Soft Computing*, 1-12.

Dang, L. M., Min, K., Lee, S., Han, D., & Moon, H. (2020). Tampered and computer-generated face images identification based on deep learning. *Applied Sciences*, *10*(2), 505.

Elaskily, M. A., Aslan, H. K., Elshakankiry, O. A., Faragallah, O. S., Abd El-Samie, F. E., & Dessouky, M. M. (2017, November). Comparative study of copy-move forgery detection techniques. In *2017 Intl Conf on Advanced Control Circuits Systems (ACCS) Systems & 2017 Intl Conf on New Paradigms in Electronics & Information Technology (PEIT)* (pp. 193-203). IEEE.

Eduard, A., & Shashkin, A. (2019). Journal of Physics: Conference Series.

Ghoneim, A., Muhammad, G., Amin, S. U., & Gupta, B. (2018). Medical image forgery detection for smart healthcare. *IEEE Communications Magazine*, *56*(4), 33-37.

Hussien, N. Y., Mahmoud, R. O., & Zayed, H. H. (2020). Deep Learning on Digital Image Splicing Detection Using CFA Artifacts. *International Journal of Sociotechnology and Knowledge Development (IJSKD)*, *12*(2), 31-44.

Huang, H., Guo, W., & Zhang, Y. (2008, December). Detection of copy-move forgery in digital images using SIFT algorithm. In *2008 IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application* (Vol. 2, pp. 272-276). IEEE.

Kim, H. J., Lim, S., Moon, J., Kim, B., & Jung, E. S. (2012). A photographic forensic case study: Myths, principles and techniques. *Mathematical and computer modelling*, *55*(1-2), 3-11..

Kashyap, A., Parmar, R. S., Agrawal, M., & Gupta, H. (2017). An evaluation of digital image forgery detection approaches. *arXiv preprint arXiv:1703.09968*.

Liu, A., Zhao, Z., Zhang, C., & Su, Y. (2017). Median filtering forensics in digital images based on frequency-domain features. *Multimedia tools and applications*, *76*(21), 22119-22132.

Meena, K. B., & Tyagi, V. (2020). A hybrid copy-move image forgery detection technique based on Fourier-

Mellin and scale invariant feature transforms. Multimedia Tools and Applications, 79(11), 8197-8212.

Mankar, S. K., & Gurjar, A. A. (2015). Image forgery types and their detection: A review. *International Journal of Advanced Research in Computer Science and Software Engineering*, *5*(4), 174-178.

Majumder, M. T. H., & Al Islam, A. A. (2018, December). A Tale of a Deep Learning Approach to Image Forgery Detection. In *2018 5th International Conference on Networking, Systems and Security (NSysS)* (pp. 1-9). IEEE.

Qureshi, M. A., & Deriche, M. (2014, February). A review on copy move image forgery detection techniques. In *2014 IEEE 11th International Multi-Conference on Systems, Signals & Devices (SSD14)* (pp. 1-5). IEEE.

Rothe, P. R., Asthankar, P. P., & Rothe, J. P. Image Forgery Detection Based on SURF and Machine Learning Classifier.

Selvaraj, P., & Karuppiah, M. (2020). Enhanced copy–paste forgery detection in digital images using scale-invariant feature transform. IET Image Processing, 14(3), 462-471.

Tembe, A. U., & Thombre, S. S. (2017, February). Survey of copy-paste forgery detection in digital image forensic. In *2017 international conference on innovative mechanisms for industry applications (ICIMIA)* (pp. 248-252). IEEE.