Implementation of Copy Paste Forgery through MATLAB

Manjot Kaur

Computer Science and Engineering,
Patiala Institute of Engineering and Technology for women, Nandpur kesho

***Abstract*: As copy-move forgery is one of the most popular image forgery so importance of forgery detection techniques is increasing day by day. Various image forgery detection techniques are proposed by researchers to withstand against several post processing operations applied over forged region but there is lot of scope in this field to search for methods which are robust to challenges like geometric transformations (scaling, rotation). Time complexity is major issue with forgery detection algorithms. Frequency-based techniques discussed in this paper are very efficient in forgery detection. These techniques can detect forgery even if blurring, noise addition and JPEG compression is used over image. Some methods are also robust to geometrical transformation.**

***Keywords*: copy-move forgery, JPEG compression, image Forgery, Copy move**

1. Introduction

Digital photo Forgery is not a stranger for human but this is a very old problem. First, it was limited to art and literature, although it did not affect ordinary people. Today, the fastest development of the internet, image processing software and the latest editing tools make this work very easy and can easily edit or modified images. In addition, it is almost impossible for human visual system to recognize whether the picture is solid or solid with a naked eye.

The digital making has improved rapidly on mainstream media and internet on the social media. By reducing the reputation of digital images, this trend shows intense sensitivity. Therefore, it is important to promote the better algorithm to verify the authenticity of digital photographs, especially considering that photographs can be used as part of medical records, news and financial documents. Therefore, in detecting photos is one of the main goals of the prime digital image forensics. The classification of image forgery is shown in Figure 1.

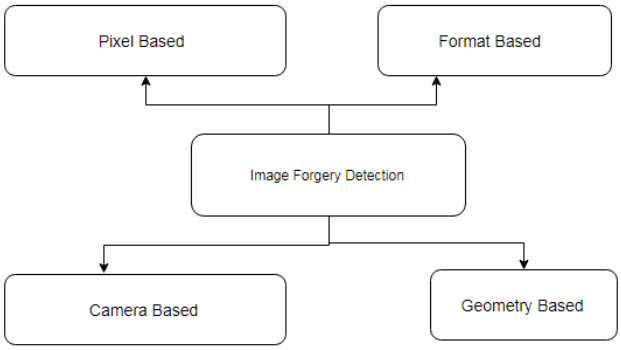

Figure 1 Types of digital image forgery techniques

1.1 Pixel-Based Image Forgery Detection

Pixel-based approach emphasis the pixels of the image. Pixel-based approach is also known as passive detection image techniques. In addition, the method is divided into four types. In this work, the photo copying image of our attention is going to forget. This technique is one of the easiest ways to fake the photos. The figure shows the ranking of image forgery modes based on 1.2 pixel. Pixel-based approach emphasis the pixels of the image. Pixel-based approach is also known as teaser detection of passive image. In addition, the method is divided into four types. In this work, the photo copying image of our attention is going to forget. This technique is one of the easiest ways to fake the photos. The figure shows the ranking of image fake modes based on 2 pixel.

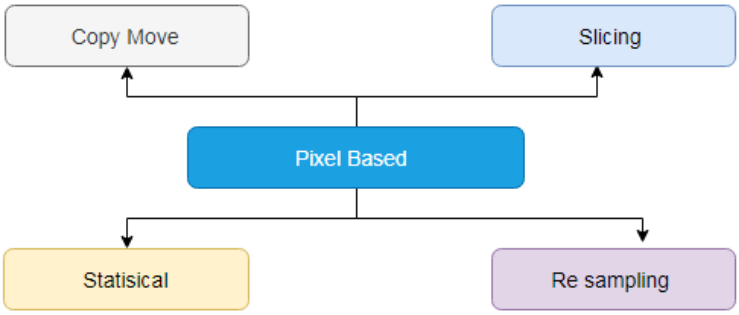

Figure 2 Pixel based image forgery

1.2 Copy-Move (Cloning)

Copy-move is widely used as well as trivial method use one of the common ways, as well known as cloning. In this type of forgery, the image or image of this image is copied and then it is shifted to one place within the image. Figure.3 presents the original picture with its doctor. The original image has a copy of six balloons and nine balloons.

Figure 3 Copy-move (cloning) image forgery

1.3 Resampling (Resize, Stretch, Rotation)

For combine two items or people, it can perform different actions, such as we have to do something or other things to match with other people. In addition, during this process, we must re-sample the original image into a new sampling lattice.

1.4 Splicing

This is a different variety of and widely used photo fake technology. In this way, two or more photos are converted into a composite image. Assume that we have two pictures, as shown in Figure 4. We collect both of them in one picture. If so careful, limitations between to identify visually.

Figure 4 Spliced image forgery

The copy - move (Cloning) Photo temperature is the most common way to tamper the image, where you copy a specific block copy or photo identification and then complete the same image in order to complete the hidden information. When the copy block comes from the same image, its special feature, noise structure and palette will be found with the rest of the image, so when we want to detect and detect it, it will become a big threat. . The poor area copy-moving (cloning) is designed to detect various methods of photographic, mainly based on block-based techniques or key point matching techniques, as in Figure 5 is shown.

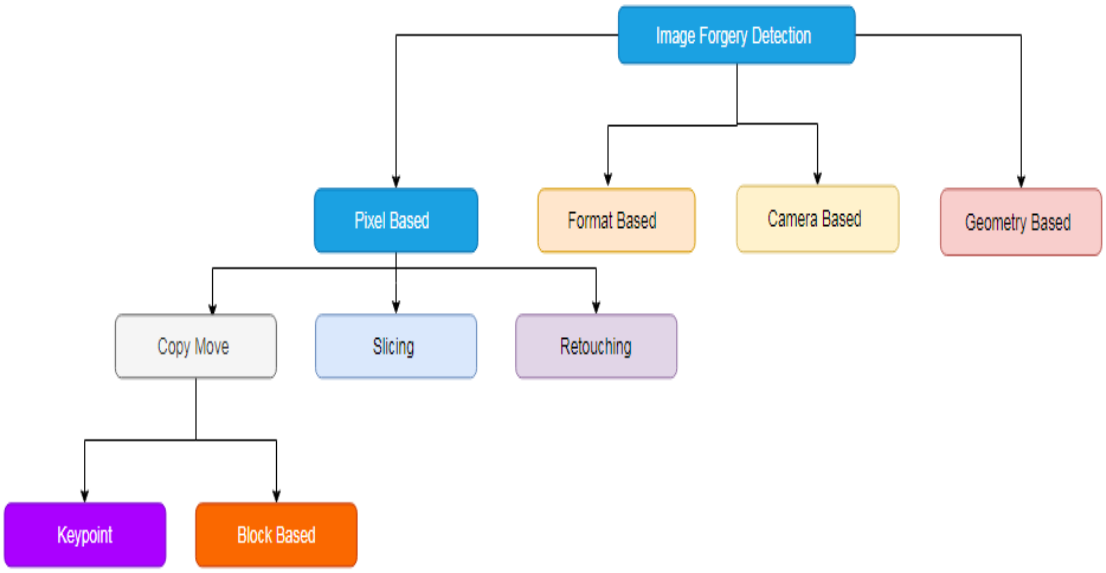

Figure 5: Image forgery detection techniques

2. Background

Manu, V. T., & Mehtre, B. M. (2016). In this era of multimedia and information blasts, thanks to the cheapest availability of software and hardware, everyone can easily capture, edit and publish photos. Unfortunately, the image editing image with intention is called tampering and can affect personal, social, economic, etc. Copy- move forgery is one of the most common and simple modes of the image display, which includes copying a picture snippet and paste it inside the same image. Its purpose may be to hide some of the pictures in the image or to hide the photo editing exhibition. In this paper, they offer new views that use maximum detection and key point detection to detect detection of cap transmission in a single picture, without the need of previous information. This experimental results obtained by testing on standard data show that the proposed procedure can bear post processing operations such as fog, JPEG compression, noise extra, and so on. In addition, their method is in detection of forgetting copy mode, where parts of the duplicate include different geographical changes such as translation, circulation and scanning.

Zandi, M., Mahmoudi-Aznaveh, A., & Talebpour, A. (2016) In this paper, they offer a novel copy - mobile maze detection plan that looks at a fairly reasonable price in the right area. For this purpose, a new point of interest is based on the benefits of block-based and traditional key-approach modes. Individually measured, key points effectively cover the whole picture, even the opposite contrast area. In addition, a new filtering algorithm is effectively used in prune area. Consider the point of view of interest, its reform strategy is proposed. Pass through this process while adjusting key density based on the information obtained. Experimental results show that the scheme offered is better than the latest method using two common benchmarked databases.

Silva, E., Carvalho, T., Ferreira, A., & Rocha, A. (2015) This work provides a new way based on digital-based multi-scale analysis and movement of voting processes - detecting mobile forgiveness. By looking at suspicious pictures, they exclude the opposite points of interest and interest in finding possible discussions between them. They cluster relevant points in geographical areas. After that, they build multiple-scale image representations, and on each scale, they use the desired characters that are strong enough to test the generated set and are strong in the compressed part, which is repeatedly reduce the search space and creates a map of detection. The final decision is based on the process of voting in all exam charts. They validated the method using various data sets containing an ancient and realistic image clone. They competed in other ways in literature with the proposed methods and promising results.

Ferreira, A., Felipussi, S. C., Alfaro, C., Fonseca, P., Vargas-Muñoz, J. E., dos Santos, J. A., & Rocha, A. (2016) The detection of copy-move image, primarily because it can misleading the process of public opinion. In this paper, they go beyond the traditional maze detectors to combine different types of movement methods of detection by cope with the problem of density behaviour, in which different techniques Output balance is ignored. Probably more than multiple scales. After that, due to liable accountability, the registration of the entry is absolutely properly estimated that the model applies to current training data. Finally, he suggested various technologies to create graphic results of ultimate results using decision making mechanisms using multi-direction data. Experimental results on the set of complicated data compare with the flexibility of detecting motion movements in literature, and other fusion modes, showing its implementation of the proposed procedure and practical applications.

Lin, H. J., Wang, C. W., & Kao, Y. T. (2009) This paper suggests a method of detecting the maze of motion movement on the flexible image by motion movement. To detect such a maze, a given picture is divided into equal size blocks, then the features of each block are extracted and represented as vectors, and then all the exclusively vector vectors Is ranked by cardinal ordering. The adjoining feature in the list is the position of each pair of vector status difference (shift vector). Estimate the total number of shaft vectors. A broader total number is considered to be a re-possibility of the region again, so all the vectors get to a wide array of

vector changes, and then their related blocks are marked to make a temporary detection result. Lastly, media filtering and component analysis is performed on temporary detection results to get final results. Compared to other modes, cardiac arresting detects more efficient without spoiling test quality.

Christlein, V., Riess, C., Jordan, J., Riess, C., & Angelopoulou, E. (2012) Forget the copy in the same image by copying and pasting and possibly moving the copy by processing. In recent years, blind image detection of a mobile bouquet copy has become the most active research subject in Forensic. Various different algorithms have been suggested, focus on processing copies after different types. In this article, their goal is how mobility - mobile fraud detection algorithm and processing phase (for example, matching, filtering, output detection, estimate of change change) Post processing is better in different scenes. Their analysis focuses on evaluating the set-up offered prefix. They offer current algorithms in public pipes. In this article, he studied the 15 most prominent feature. They analyzed the performance of each image and every pixel. They created real-time copy mobile data sets and software frameworks for processing system image. Experiments show SHIFT and SURF, that block-based DCT, DVD, KP, PCA, PCA, and ZERNIKE functions are the best for key-based safety and surf safety functions. This feature set is a better source than a better source of sources and reliably identify in the trafficking areas.

He, Z., Lu, W., Sun, W., & Huang, J. (2012) Image stitch is very common in the picture and image-tampering image. To restore the confidence of people in digital photos, it is necessary to detect photo stitching. In this paper, a mark-based method is presented to detect this specific architecture. First of all, the characteristics of the original mark of Shia and L-created attributes in the DCT domain generated by Matrix. Expansion is not only to block inter blocks between the blocks inside the block but also the block of DCT dynamic elements. After that, more features are built in DWT domains so that the ground, three-dimensional features of the wave in position, scale and direction. After that, the field selection method is used to meet the task of reducing the SVM-RFE feature, making it easier for calculating cost. Finally, the real and slow images are the final dimensions of the final dimension featured by the feature vector via the support vector machine (SVM). Experienced results show that the method offered can delete some of the advanced methods.

Al-Qershi, O. M., & Khoo, B. E. (2013) Currently, digital photos and videos are extremely important because they become important information about the information. However, it is easy to tamper with photos and videos that their authenticity is not reliable. Digital Photo forensics solves image verification or problem by it. One of the main branches of the photo phoenix is to detect inactive image forgiveness. Images can be fake using different techniques, the duplicate movement of the most common forgiveness, where the picture area is copied and placed in the same picture in the second picture. Active techniques have been presented as water exhibitions to solve image reliability problems, but their techniques are limited because they require human interference or especially equipped cameras. In order to overcome these limits, many inactive verification methods have been suggested. No pre-related information about the image is needed in a passive way of active function, and they can carry detectable changes in image-specific changes using fake things. In this article, she describes the current state of art in passive duplicate-detection methods of detection. Then, to address these issues, the powerful trend indicates key current issues to promote detectors with detectors and address trends.

Birajdar, G. K., & Mankar, V. H. (2013) Today, digital image processing has been made easy for powerful computers, advanced image editing software packages and high-resolution capture devices. Image integrity validation and without any need for additional image material is an important area of researching any previous knowledge of trapped marks or embedded water marks. Trying a complete Bible offer to investigate the latest progress in the field of digital image maze detection and to detect fake detection of detective detection. No clear offer is required for the image of blending or inactive ways. First of all, different image fake detection techniques are ranked and are generally developed in the structure. An overview of the validation of the inactive picture is introduced, and current blind maze detection techniques are reviewed. For future research, the current status of image forgery detection technology is discussed along with a recommendation for future research.

3. Simulation

Digital image forgery detection is a technology that is used to detect whether an image is manipulated or not. There are various ways to manipulate an image e.g. copy-move forgery, image splicing, image retouching etc. Therefore, the task of detecting a forged image is very complex. Hence, the approach to handle and detect different types of forgery is different. Among the various types of image tampering approach, copy-move is widely and commonly used. In copy-move image forgery a part of image is copied and then it is pasted in the same image having an intention to make a false image or hide some important object within the image. There are a number of copy-move image forgery detection algorithms but most of them are not robust and efficient in terms of computational expanse and affine or geometric transformation. The goal of this proposed method is to detect forgery irrespective of all the ways of copy-move tampering including the tampering with geometric transformation with giving importance on the reduction issue of time complexity.

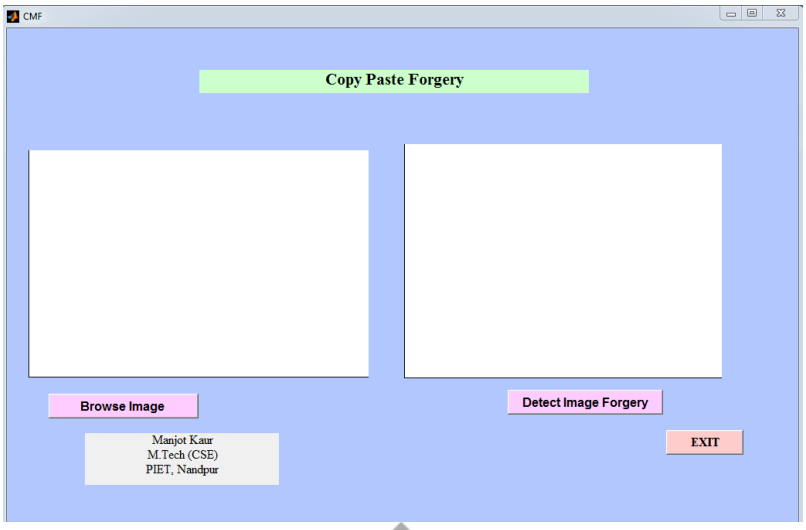

Figure 6. Project Layout of Copy Paste Forgery Project

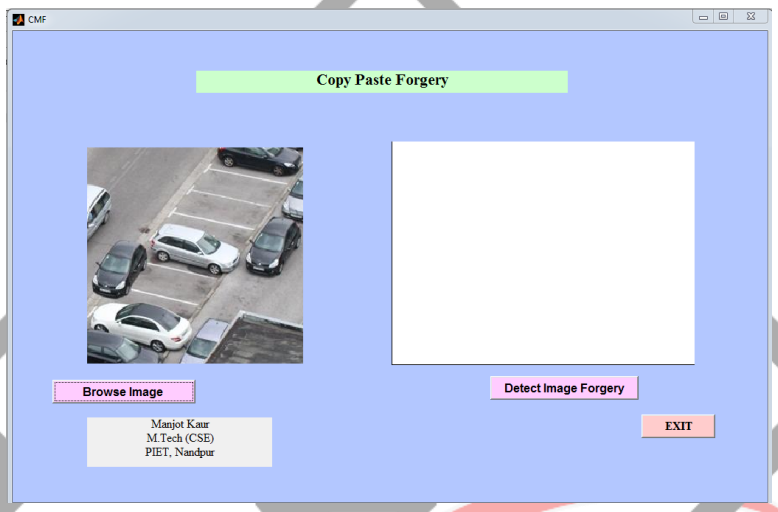

Figure 7. Browse forced image

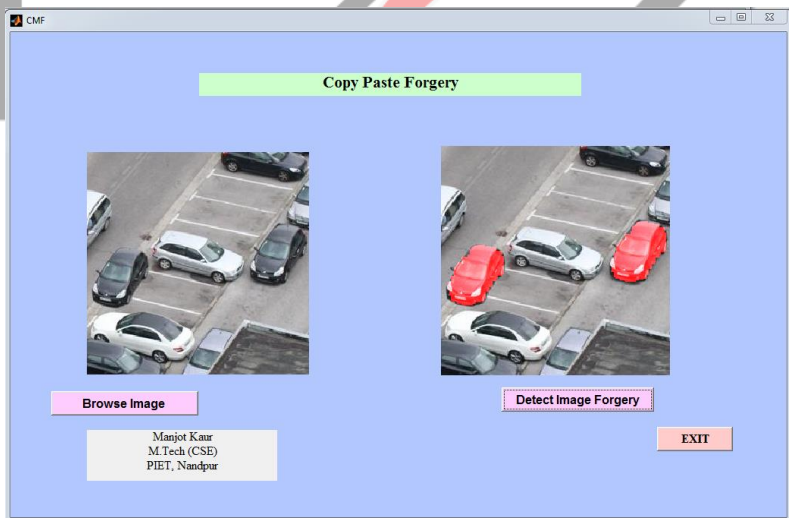

Figure 8. Detected forced image

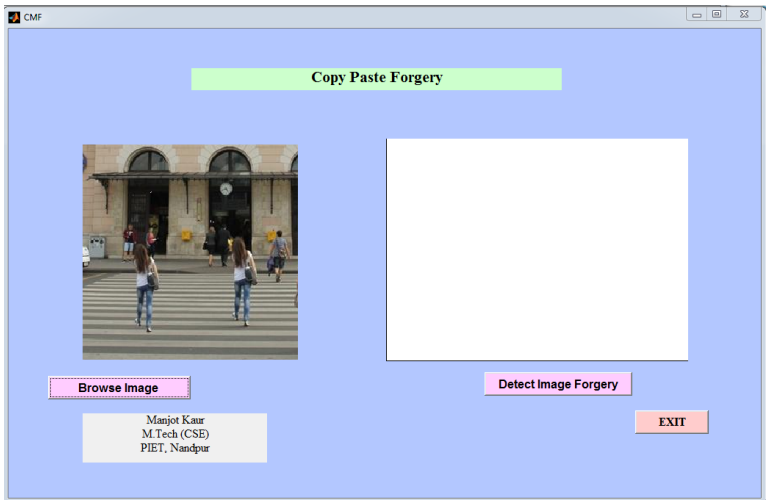

Figure 9. Browse forced image

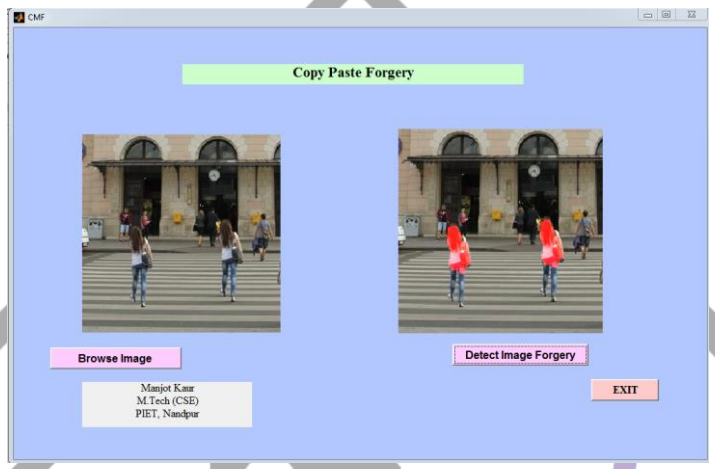

Figure 10. Detected forced image

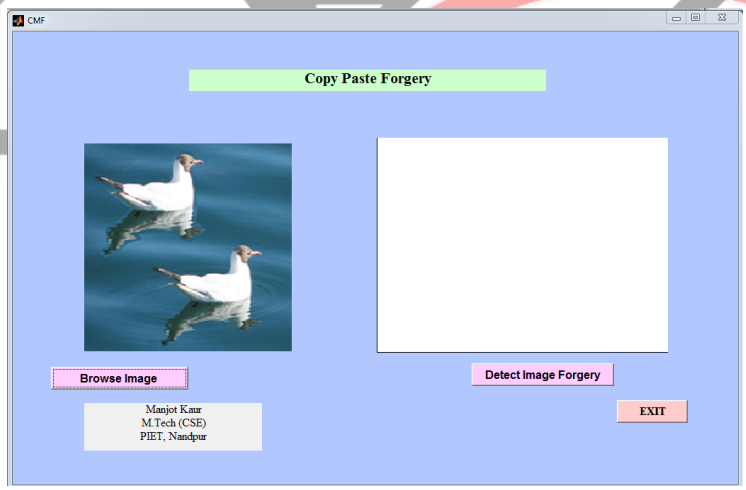

Figure 11. Browse forced image

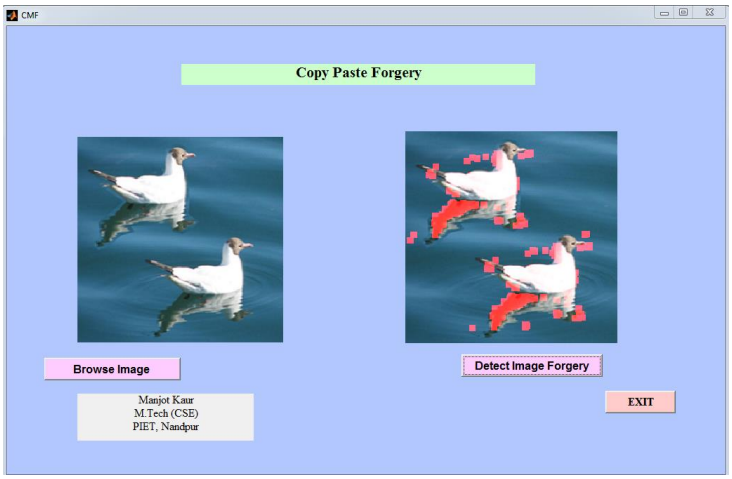

Figure 12. Detected forced image

Figure 13. Browse forced image

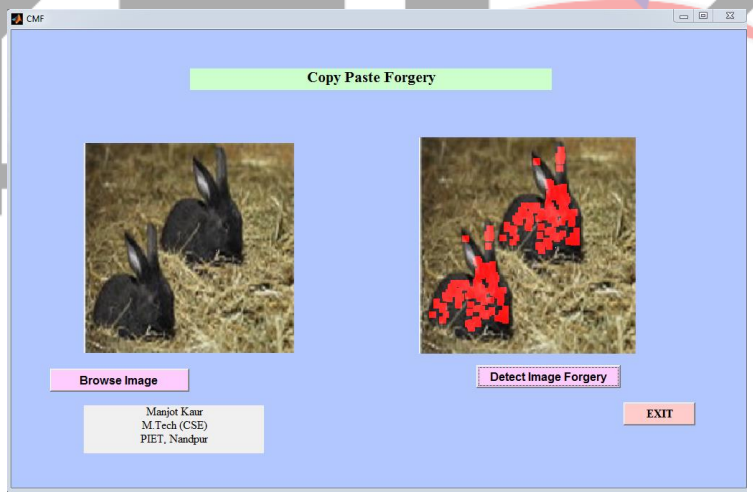

Figure 14. Detected forced image

4. Conclusion and Future Work

With the rapid progress of image processing technology, detection of digital image forgery is an interesting research topic in forensic science. We can consider the specific type of image tampering as a "copy paste forgery", which is one of the emerging problems in the field of digital image forensic. In copy-move forgery method a part of original digital image is copied and pasted to another part in the same original image to make it, as a forged one. An effective detection of specific copy-paste type of image tampering has been proposed in this thesis. In this thesis, we show that our process is useful to identify the copy-paste region. The proposed method can detect duplicated region from all sample images. In the future, we would like to detect other types of image files and enhance performance of the proposed detection.

References

[1] Cozzolino, D., Poggi, G., & Verdoliva, L. (2015). Efficient dense-field copy–move forgery detection. *IEEE Transactions on Information Forensics and Security*, *10*(11), 2284-2297.

[2] Ardizzone, E., Bruno, A., & Mazzola, G. (2015). Copy–move forgery detection by matching triangles of keypoints. *IEEE Transactions on Information Forensics and Security*, *10*(10), 2084-2094.

[3] Warif, N. B. A., Wahab, A. W. A., Idris, M. Y. I., Ramli, R., Salleh, R., Shamshirband, S., & Choo, K. K. R. (2016). Copy-move forgery detection: survey, challenges and future directions. *Journal of Network and Computer Applications*, *75*, 259-278.

[4] Zhu, Y., Shen, X., & Chen, H. (2016). Copy-move forgery detection based on scaled ORB. *Multimedia Tools and Applications*, *75*(6), 3221-3233.

[5] Yang, F., Li, J., Lu, W., & Weng, J. (2017). Copy-move forgery detection based on hybrid features. *Engineering Applications of Artificial Intelligence*, *59*, 73-83.

[6] Manu, V. T., & Mehtre, B. M. (2016). Detection of copy-move forgery in images using segmentation and SURF. In *Advances in signal processing and intelligent recognition systems* (pp. 645-654). Springer, Cham.

[7] Zandi, M., Mahmoudi-Aznaveh, A., & Talebpour, A. (2016). Iterative copy-move forgery detection based on a new interest point detector. *IEEE Transactions on Information Forensics and Security*, *11*(11), 2499-2512.

[8] Silva, E., Carvalho, T., Ferreira, A., & Rocha, A. (2015). Going deeper into copy-move forgery detection: Exploring image telltales via multi-scale analysis and voting processes. *Journal of Visual Communication and Image Representation*, *29*, 16-32.

[9] Ferreira, A., Felipussi, S. C., Alfaro, C., Fonseca, P., Vargas-Muñoz, J. E., dos Santos, J. A., & Rocha, A. (2016). Behavior knowledge space-based fusion for copy–move forgery detection. *IEEE Transactions on Image Processing*, *25*(10), 4729-4742.

[10] Lin, H. J., Wang, C. W., & Kao, Y. T. (2009). Fast copy-move forgery detection. *WSEAS Transactions on Signal Processing*, *5*(5), 188-197.

[11] Christlein, V., Riess, C., Jordan, J., Riess, C., & Angelopoulou, E. (2012). An evaluation of popular copy-move forgery detection approaches. *IEEE Transactions on information forensics and security*, *7*(6), 1841-1854.

[12] He, Z., Lu, W., Sun, W., & Huang, J. (2012). Digital image splicing detection based on Markov features in DCT and DWT domain. *Pattern Recognition*, *45*(12), 4292-4299.

[13] Al-Qershi, O. M., & Khoo, B. E. (2013). Passive detection of copy-move forgery in digital images: State-of-the-art. *Forensic science international*, *231*(1-3), 284-295.

[14] Birajdar, G. K., & Mankar, V. H. (2013). Digital image forgery detection using passive techniques: A survey. *Digital investigation*, *10*(3), 226-245.