# ENHANCED DOMINATED COMPLETED MEDIAN TERNARY PATTERN
# FOR DETECTION OF COPY-MOVE IMAGE FORGERY
# AGAINST POST-PROCESSING OPERATIONS

RAFIDAH BINTI MUHAMAD

A thesis submitted in fulfilment of the
requirements for the award of the degree of
Master of Philosophy

School of Computing
Faculty of Engineering
Universiti Teknologi Malaysia

DECEMBER 2020

# DEDICATION

This thesis is dedicated to my father and mother who believe in me. To my friends who struggled with me along the journey, who went for vacation to help me get rid of stress, who always be there when needed, who called me just to check my whereabouts, who will be with me on the stage later. To me, myself, and I.

# ACKNOWLEDGEMENT

In preparing this thesis, I was in contact with many people, researchers, academicians, and practitioners. They have contributed towards my understanding and thoughts. I wish to express my sincere appreciation to my main thesis supervisor, Dr. Azurah Binti A Samah for encouragement, guidance, critics, and support. I am also very thankful to my co-supervisor Mr. Hairudin Bin Abdul Majid for his guidance, advice, and motivation. My appreciation also goes to Professor Dr. Ghazali Bin Sulong for introducing me with this field in the first place. Without their continued support and interest, this thesis would not have been the same as presented here.

I am also indebted to Universiti Teknologi Malaysia (UTM) for funding my research under GUP Research Grant (Grant Number: Q.J130000.2528.19H17) and Yayasan Khazanah for funding my Master of Philosophy research.

My fellow postgraduate students should also be recognised for their support. My sincere appreciation also extends to all my colleagues and others who have helped at various occasions. Their views and tips are useful indeed. Unfortunately, it is not possible to list all of them in this limited space. I am grateful to all my family members.

# ABSTRACT

Copy-move forgery which is an act of copying an object and pasting it on another location of the same image is one of the most common types of tampering techniques to manipulate image content. Besides, most of the images are also being tampered by post-processing operations such as JPEG compression, contrast adjustment, brightness change, colour reduction, noise addition, and blurring before pasted, makes it more challenging to detect, as found in the standard dataset CoMoFoD. In multimedia forensics, many efforts have been undertaken to detect whether an image is pristine or manipulated by proposing various techniques to improve the robustness of these detection methods. However, researchers continue to face challenges in detecting tampered region with the presence of all these post-processing attacks in a copy-move image forgery and relatively few methods were attempted to address them. The main objective of this research is to design and develop an improved descriptor with features invariance to post-processing operations for copy-move forgery detection. Generally, image processing steps consist of four main steps which are pre-processing, feature extraction, block matching and evaluation of results. In this process, an improvement is made by employing sign operator for feature extraction with mean (robust) as threshold to extract invariance feature vectors against post-processing attacks from each block of image. An Euclidean distance is employed to filter out the weak features and obtain rough suspected matches. The results obtained were very encouraging with Correct Detection Rate (CDR) of more than 99% achieved for the normal tampered images, while the ones with post-processing operations fluctuated between 91% and 99.7%. The results have proven that the proposed copy-move forgery detection performed better than the existing techniques.

# ABSTRAK

Pemalsuan salinan-pindaan yang merupakan tindakan menyalin objek dan menampalnya di lokasi lain dari imej yang sama adalah salah satu jenis teknik pemecatan yang paling biasa untuk memanipulasi kandungan imej. Selain itu, kebanyakan imej juga diganggu oleh operasi pasca pemprosesan seperti pemampatan JPEG, pelarasan kontras, perubahan kecerahan, pengurangan warna, penambahan bunyi, dan kabur sebelum ditampal, menjadikannya lebih mencabar untuk dikesan seperti yang terdapat di dalam dataset standard CoMoFoD. Dalam forensik multimedia, banyak usaha dilakukan untuk mengesan sama ada imej itu murni atau dimanipulasi dengan mencadangkan pelbagai teknik untuk meningkatkan keteguhan kaedah pengesanan ini. Walau bagaimanapun, para penyelidik terus menghadapi cabaran dalam mengesan rantau yang mengalami kerosakan dengan kehadiran semua serangan pasca pemprosesan ini dalam pemalsuan imej salin dan agak relatif dengan kaedah yang cuba ditangani. Objektif utama kajian ini adalah untuk mereka bentuk dan membangunkan deskriptor yang lebih baik dengan ciri-ciri keupayaan untuk operasi pasca-pemprosesan untuk pengesanan pemalsuan pemindahan salinan. Secara amnya, langkah memproses imej terdiri daripada empat langkah utama iaitu pra-pemprosesan, pengekstrakan ciri, padanan blok dan penilaian hasil. Dalam proses ini, penambahbaikan dibuat dengan menggunakan pengendali tanda untuk pengekstrakan ciri dengan nilai min (teguh) sebagai ambang untuk mengekstrak vektor ciri *invariance* terhadap serangan pasca pemprosesan dari setiap blok imej. Jarak *Euclidean* digunakan untuk menyaring ciri-ciri yang lemah dan mendapatkan perlawanan yang disyaki kasar. Hasil yang dicapai sangat menggalakkan dengan Kadar Pengesanan yang Benar (CDR) melebihi 99% yang dicapai untuk imej tamparan yang normal, manakala yang dengan operasi pasca pemprosesan bervariasi antara 91% dan 99.7%. Hasilnya telah membuktikan bahawa cadangan pengesanan pemalsuan salinan yang bergerak lebih baik daripada teknik yang ada.

## TABLE OF CONTENTS

## LIST OF TABLES

## LIST OF FIGURES

# LIST OF ABBREVIATIONS

| | | |
|---|---|---|
| JPEG | - | Joint Photographic Experts Group |
| CMFD | - | Copy-Move Forgery Detection |
| DCMTP | - | Dominated Completed Median Ternary Pattern |
| LBP | - | Local Binary Pattern |
| SIFT | - | Scale Invariant Feature Transform |
| SURF | - | Speeded up Robust Features |
| SNR | - | Signal-to-Noise Ratio |
| QEM | - | Quaternion Exponent Moments |
| PCA | - | Principal Component Analysis |
| SVD | - | Singular Value Decomposition |
| SWT | - | Stationary Wavelet Transform |
| MLBP | - | Multi-Resolution Local Binary Pattern |
| RANSAC | - | RANdom SAmple Consensus |
| LTP | - | Local Ternary Pattern |
| DLBP | - | Dominated Local Binary Pattern |
| CLBP | - | Completed Local Binary Pattern |
| CLTP | - | Completed Local Ternary Pattern |
| k-d tree | - | k dimensional tree |
| CDR | - | Correct Detection Rate |
| ANN | - | Approximate Nearest Neighbour |
| ED | - | Euclidean Distance |
| SV | - | Shift Vector |
| FDR | - | False Detection Rate |

# LIST OF SYMBOLS

| | | |
|---|---|---|
| $t$ | - | Dynamic ternary threshold |
| $CV$ | - | Coefficient of variation |
| $MAD$ | - | Median of the absolute deviations |
| $\mu$ | - | Mean of block pixels |
| BxB | - | Size of overlapping block |
| $\sigma$ | - | Standard deviation of block value |
| TB | - | Total number of overlapping blocks |
| $g_c$ | - | Grey value of centre pixel of cell |
| $g_p$ | - | Grey value of the neighbour pixels of cell |
| $Y$ | - | Luminance component |
| MxN | - | Size of tampered image |
| $g_{med}$ | - | Grey value of median pixel of cell |
| $\bar{x}_R$ | - | Mean robust |

# LIST OF APPENDICES

# CHAPTER 1

# INTRODUCTION

## 1.1 Overview

Rapid evolvement in information technology set the stage for more technological evolution. Primarily, information has been passed using word, but it has been replaced by image where it can convey better information especially in the field of crime, journalism, etc. However, the concern is that there is a high potential of vicious forgery where digital images can be changed to hide the truth by using various image editing tools such as Photoshop which is very easy to use even by beginners.

Thajeel (1) stated that photographers in the early-to-mid 20th century had realised that image forgeries could be powerful tools for changing public perception and even history. For instance, in (2), a photo on Facebook that shows a crowd of supporters of former Malaysia’s Prime Minister , Najib Razak, is considered as fake one because obviously, the crowd has been duplicated to appear larger (see Figure 1.1).

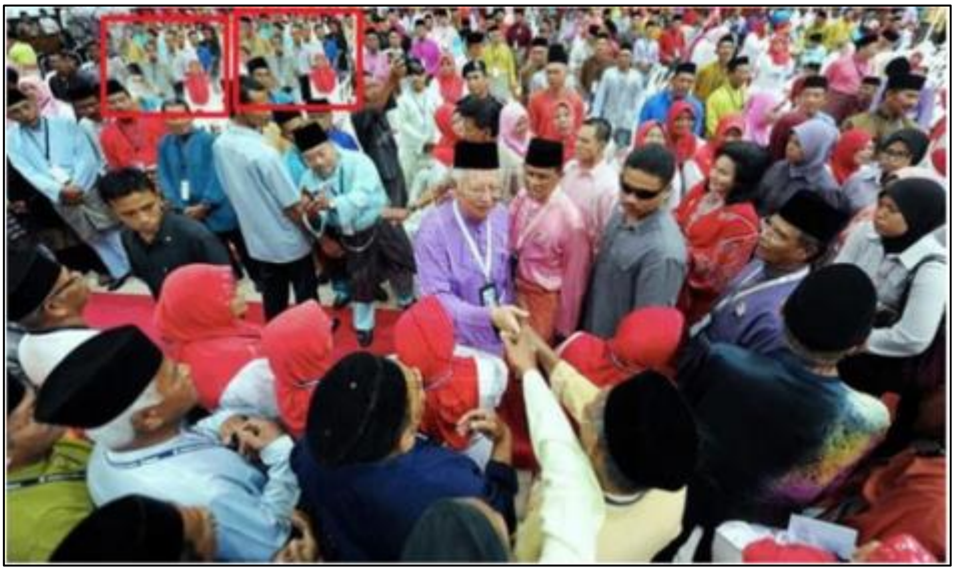


Figure 1.1 An example of fake photo (2)

In the field of image forgery, there are several types of forgery that have been investigated such as copy-move, splicing, and morphing. However, Copy-Move Forgery (CMF) is the most actively investigated subtopic of digital image forgery where some objects are being cloned in the same image (3–5). Even though it is known that the level of difficulties for detection of copy-move image forgery is very high as the duplicated region has almost similar characteristics in terms of texture, noise, and colour, however, previous researchers had proved that some methods able to detect the forged region by using the fact that the forging operation results in certain non-uniformities introduced into the image that can be used to detect the forgery(3,5).

## 1.2 Problem Background

Copy-move is known as one of the most common method for image forgery (6). Besides, to make it worse, most of the forged images does not forged by solely copy-move, either by single or multiple forged regions, but also being forged by attacks. These attacks which categorized into two are called post-processing operations and geometric transformations, added before copied region is pasted on the image, making the process of detecting forged region more challenging (7). Most of the related works on the Copy-Move Forgery Detection (CMFD) were however focused on correct detection rate of forged image in the presence of geometric transformations and certain post-processing operations only (8). Limited works dealt with correct detection rate for all post-processing operations mentioned even though they are available in the standard dataset, CoMoFoD (1,9).

Joint Photographic Experts Group (JPEG) compression (8), contrast adjustment (10), brightness changes (11), colour reduction (1), Gaussian additive noise, and blurring are among the example of post-processing operations. Tralic *et al*. (12) created a CoMoFoD database that has 200 image sets in size 512x512 pixels of these operations for detection purpose. This research will use first 40 images from the database where these images contain a copied region which had been translated to the new location with post-processing operations.

For JPEG compression, images in the database are processed with different quality factors from 20 until 90 with increment of 10. The lowest quality factor degrades the forged image and make it more imperceptible when compared to the other quality factors as a low-quality factor directly impacts the visual quality of the image and results in a smaller JPEG file. From a viewpoint of detecting forgery, another impact from quality is low-quality images can reduce the ability to detect modifications.

For noise addition, images in the database are processed with different variance viz., [0.009, 0.005, 0.0005]. Noise can significantly influence the quality of digital images. This results in a granular texture added to the image. The image is however significantly smoothed, and the edges significantly blurred. The image which have been post-processed with first level 0.009 is more imperceptible since high variance of noise randomly corrupts the image. From a forensic viewpoint, hiding information in the image can have a very high percentage of being unnoticed.

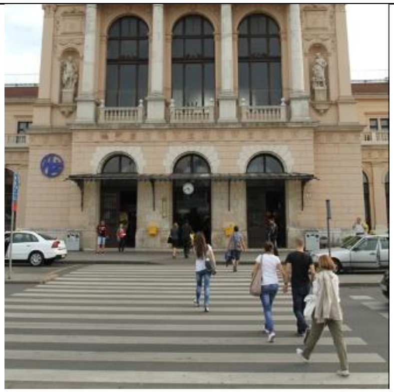
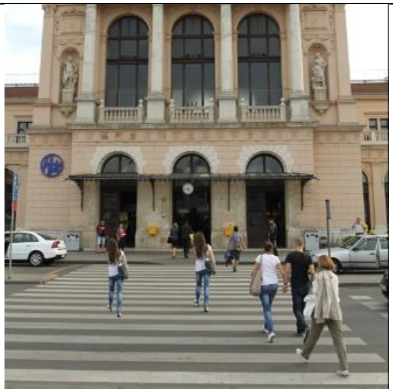
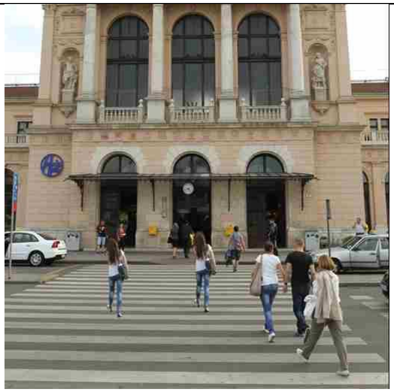
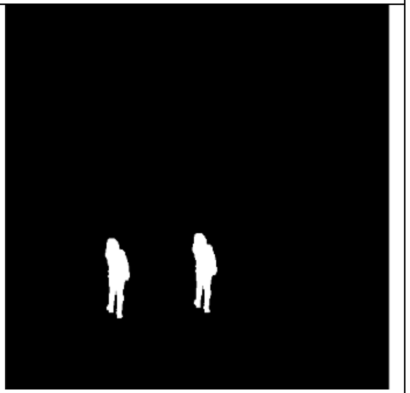
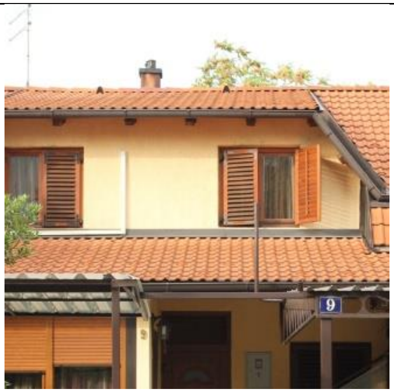
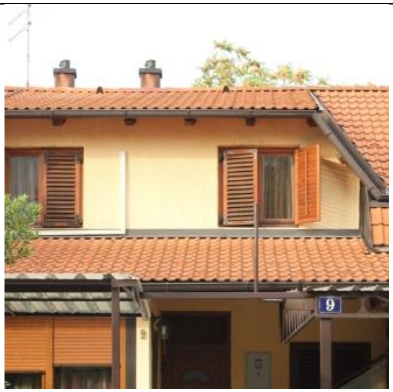
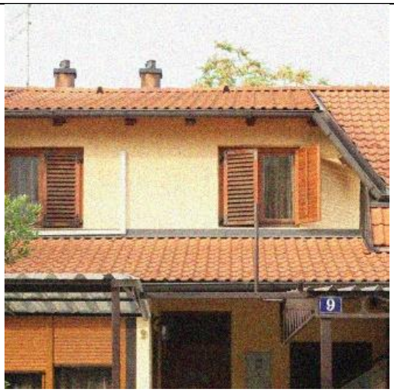
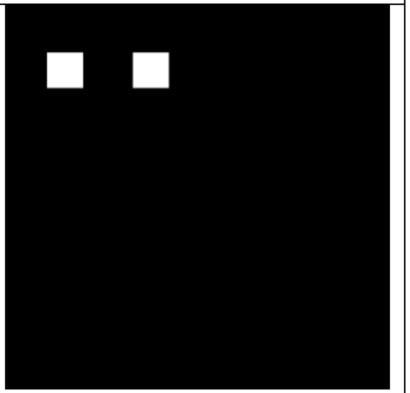
For blurring operation, images in the database are processed by making the colour transition from one side of an edge in the image to another smoothly using three different filter masks to obtain blurred images. These masks are considered as a rectangular group of pixels surrounding the pixel of image called the kernel with average filters of size 3x3, 5x5 and 7x7. To apply this filter to the current pixel, a weighted average of the colour values of the pixels in the kernel is calculated. This averaging is done on a channel-by-channel basis, and the average channel values become the new value for the filtered pixel. The effect is to average out rapid changes in pixel intensity. In CoMoFoD, the kernel with a dimension of seven pixels degrades the forged image much than the other dimensions. This is because larger kernel has more values factored into the average, and this implies that a larger kernel will blur the image more than a smaller kernel.

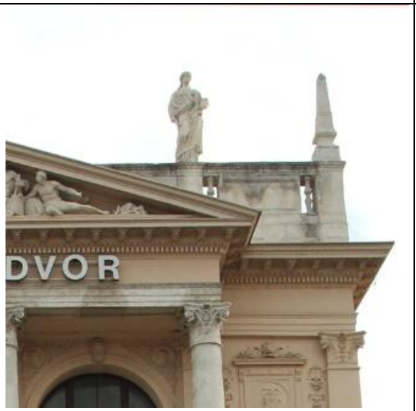
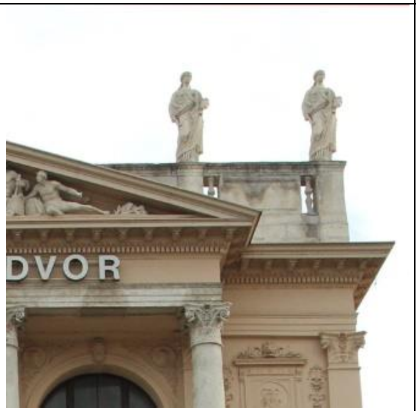
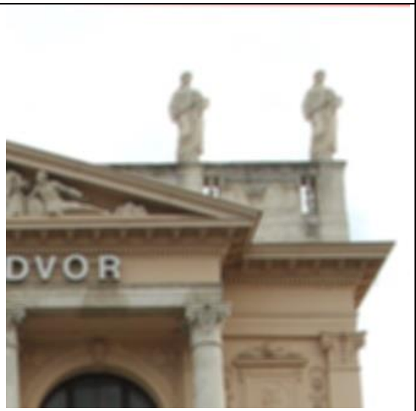
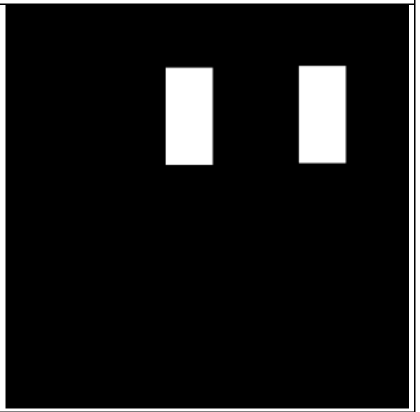
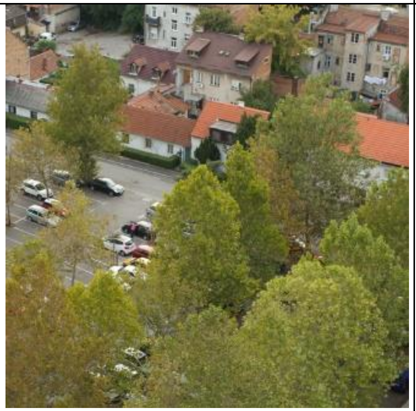
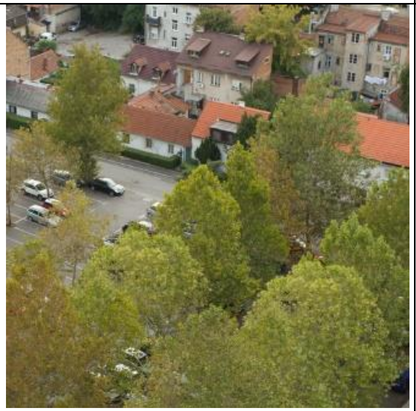
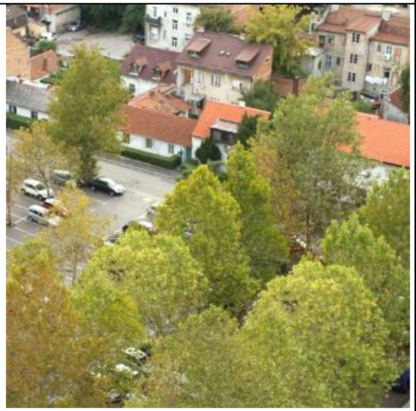
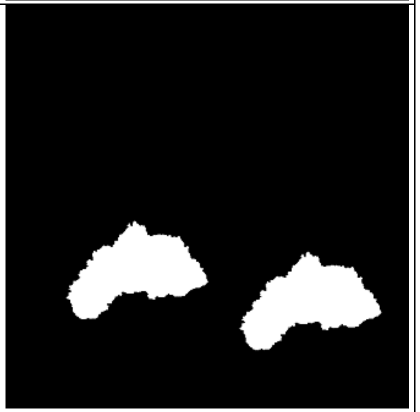
The brightness and contrast of an image can be adjusted by changing the value of all pixels by a constant. For these two operations, images in the database are processed with different levels with lower and upper bounds viz., [(0.01, 0.95), (0.01, 0.9), (0.01, 0.8)]. The image with intensity value of [0.01,0.80] are significantly different on appearance as it is brighter (brightness) and darker (contrast) thus making it more imperceptible. For brightness changes, lower value of upper bounds [0.01, 0.80] changes the image to be brighter whereas higher value of upper bounds changes the image to be darker [0.01, 0.95]. Meanwhile, for contrast adjustment, values from the lower and upper bounds create a window which reduces contrast when stretching the window [0.01, 0.95] while increases contrast when shrinking the window [0.01, 0.80].

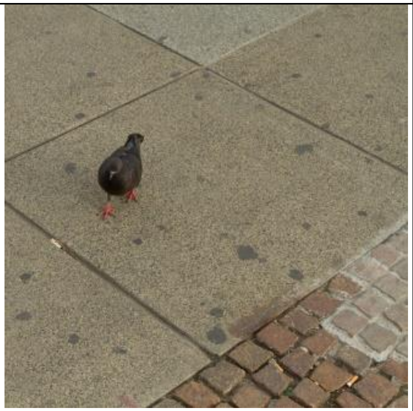
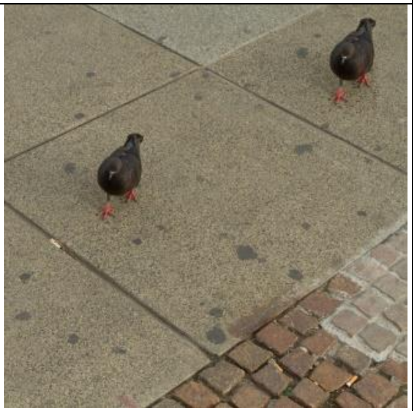
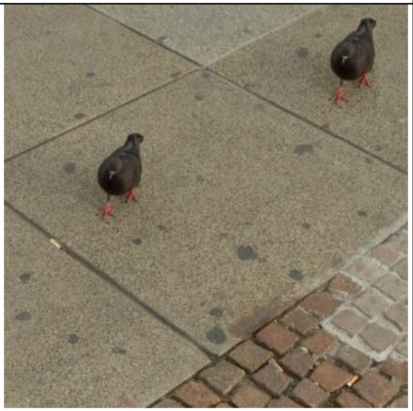
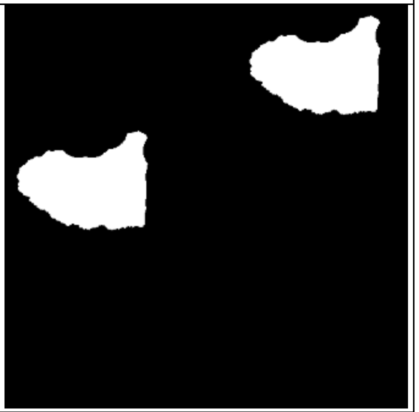
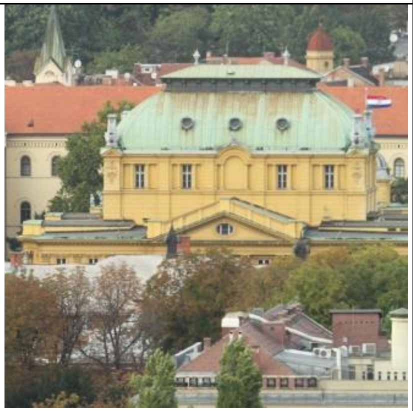
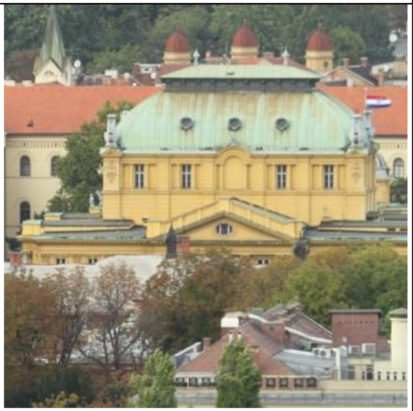
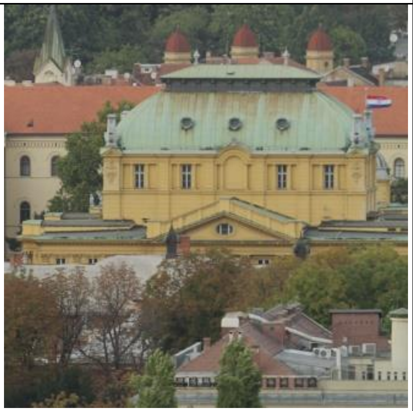
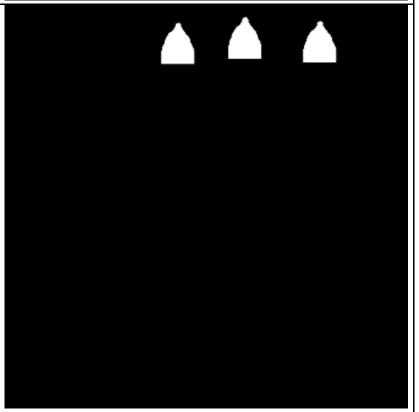
The process of colour reduction happens by replacing every colour of the original image by an appropriate colour from the limited number of colours available. The effect was unfortunately resulting in image discolouration. In CoMoFoD database, images are processed with different level of colour quantization from 256 to 128, 256 to 64 and 256 to 32. Third level of quantization 32 is visually imperceptible when compared to the other two levels as the image is represented with a smaller number of colours.

Table 1.1 shows the example of original image and the image with stated operations.

Table 1.1 Example of original image and forged image with post-processing operations in CoMoFoD database (1,12)

| Type of Post-Processing Operations | Original Image | Normal Forged Image | Forged Image with Post-processing Operations | Ground Truth |
|---|---|---|---|---|
| JPEG Compression |  |  |  |  |
| Noise Addition |  |  |  |  |

| Type of Post-Processing Operations | Original Image | Normal Forged Image | Forged Image with Post-processing Operations | Ground Truth |
|---|---|---|---|---|
| Blurring |  |  |  |  |
| Brightness Changes |  |  |  |  |

| Type of Post-Processing Operations | Original Image | Normal Forged Image | Forged Image with Post-processing Operations | Ground Truth |
|---|---|---|---|---|
| Colour Reduction |  |  |  |  |
| Contrast Adjustment |  |  |  |  |

## 1.3 Problem Statement

Feature extraction which extracts an appropriate feature from each of the blocks or interesting pixels is a core phase in the CMFD scheme. Therefore, a good feature extraction method is needed to generate invariance feature vectors and get high Correct Detection Rate (CDR) of forged image. CDR is calculated by comparing each pixel found in the detected tampered block with the ground truth. If the pixel exists in both blocks, then the pixel is counted as the correctly detected pixel. Otherwise, it is considered as wrongly detected pixel. In feature extraction, the closer CDR to 1 and False Detection Rate (FDR) to 0, the higher is the method's precision.

Based on the above challenges, there are two issues that need to be answered. The first issue is to improve the CDR of the proposed method against single and multiple forged regions distorted by various post-processing operations and the second issue is to handle outlier that may affect the results of CDR obtained in. Despite the accomplishments obtained by the previous studies involving post-processing operations on copy-move forgery image, it is discovered that many existing feature extraction methods are limited to certain type of operations only (8). This is because the specific threshold value determination only valid for certain operations and not to others thus, results in generation of variance features vector that led to low CDR.

The inability to generate invariance feature vectors against all type of operations has resulted in incorrect localization of duplicated object during the matching stage. In pattern recognition, the ability to extract invariance features from an image is important. An invariance feature vectors are vectors extracted from image where they can be identified independently of its position, size, and orientation. Generally, they are vectors which remain unchanged under certain transformations. In this study, invariance features vector are vectors which remain unchanged under the presence of post-processing operations.

It is worth noting that the Completed Local Binary Pattern-Sign (CLBP-Sign or CLBP_S) in Completed Local Binary Pattern (CLBP) and Completed Local Ternary Pattern (CLTP) is equivalent to the conventional Local Binary Pattern (LBP) (13) in terms of noise sensitivity caused by a static threshold, which is obtained from the centre pixel. Hence, the creation of a noise insensitive threshold and monotonic greyscale transformation invariance is mandatory. Following that, (1) proposed a method called Dominated Completed Median Ternary Pattern (DCMTP) which based on similar CLTP principles but differed in terms of the thresholding approach.

This study proved that even with a presence of post-processing operation, DCMTP able to produce high CDR. This is because DCMTP employs two new thresholds namely, median-based threshold and dynamic ternary threshold. The former can perform well in the presence of noise while the latter can perform well in the presence of noise and other post-processing operations such as blurring, brightness, JPEG compression and colour reduction.

Although being able to perform well against noise, unfortunately, noise can significantly influence the quality of digital images resulting in low CDR of forged region for images which have been post-processed with first level 0.009 since the high variance of noise randomly corrupts the image. Besides, the method had limitation in getting the CDR as high as the other operations when facing JPEG compression operation especially for the forged image with a very low-quality factor 20.

Therefore, this research will propose a new threshold for feature extraction namely, mean (robust) that able to overcome the limitation exist by using median-based threshold as well as reducing the impact of outliers (14). While the arithmetic mean is often used to report central tendencies, it is not a robust statistic, meaning that it is greatly influenced by outliers (values that are very much larger or smaller than most of the values). Usually, the outlier is removed from the data set for further analysis which reduces the degrees of freedom. The results obtained when using mean robust reveal that the proposed mean is less affected by the outlier than the arithmetic mean.

## 1.4 Research Goal

This research aims to develop an improved method with features invariance to post-processing operations for copy-move forgery detection.

### 1.4.1 Research Objectives

The objectives of this research are specified as follows:

i. To propose an improved Dominated Completed Median Ternary Pattern (DCMTP) method that can extract features invariance to post-processing operations.

ii. To use outlier analysis to test the results and analyse the overall dataset and environment to be sure on the effect of outliers' presence towards the correct detection rate (CDR).

## 1.5 Scopes

The scopes of this research are as follow:

(a) This research utilizes the CoMoFoD standard and completed dataset (www.vcl.fer.hr/comofod/) by (12) throughout the CMFD process. The forged images that been used undergone shifting of copied regions only.

(b) The proposed method is categorized under the group of block-based methods.

(c) This research uses block overlapping technique for image partitioning.

(d) This research places emphasis on the correct detection rate of the proposed method in copy-move image forgery detection.

## 1.6 Research Significance

The significance of this research is that the proposed CMFD method able to overcome the challenges of post-processing operations existed in forgery detection. The proposed CMFD may do so by reducing the impact of the operations by extracting robust feature that is invariance to the operations.

Besides, this research can provide a method that can authenticate an originality of an image either being normally copy and pasted or had being concealed by operations to hide the traces of tampering. Although there are many previous studies regarding CMFD that have shown many encouraging results, however, they are still limitation in the challenges mentioned above especially in the presence of multiple copy-move forgeries.

In addition, this research shows that with the high quality or efficient choice of threshold in the feature extraction phase, enabling the scheme to reduce a phase which is the post-processing phase, thus reducing the processing time to execute the whole detection process.

## 1.7 Thesis Organization

This thesis is arranged into six chapters as follows:

Chapter 2 presents an overview of copy-move forgery, existing works on feature extraction from forged images with various post-processing attacks in single and multiple forgeries and issues on false positive as well as the limitations in previous research.

Chapter 3 describes the research framework that supports the objectives of the research.

# REFERENCES

1. Thajeel SA. Copy-move Image Forgery Detection Scheme Based on New Texture Descriptor Utilising Graphical Processing Unit. Universiti Teknologi Malaysia, Johor, Malaysia; 2016.
2. Abdel-Basset M, Manogaran G, Fakhry AE, El-Henawy I. 2-Levels of clustering strategy to detect and locate copy-move forgery in digital images. Multimed Tools Appl. 2018;1–19.
3. Ardizzone E, Bruno A, Mazzola G. Copy – Move Forgery Detection by Matching Triangles of Keypoints. IEEE Trans Inf Forensics Secur. 2015;10(10):2084–94.
4. Bi X, Pun CM, Yuan XC. Multi-Level Dense Descriptor and Hierarchical Feature Matching for Copy-Move Forgery Detection. Inf Sci (Ny). 2016;345:226–42.
5. Kumar M, Srivastava S. Image forgery detection based on physics and pixels: a study. Aust J Forensic Sci [Internet]. 2017;0618(August):1–16. Available from: https://www.tandfonline.com/doi/full/10.1080/00450618.2017.1356868
6. Prakash CS, Maheshkar S, Maheshkar V. Detection of copy-move image forgery with efficient block representation and discrete cosine transform. Srivastava S, Malik H, Sharma R, editors. J Intell Fuzzy Syst [Internet]. 2018 Nov 20 [cited 2019 Jan 30];35(5):5241–53. Available from: https://www.medra.org/servlet/aliasResolver?alias=iospress&doi=10.3233/JIFS-169808
7. Sharma S, Ghanekar U. Dominating direction based an efficient copy–move image tampering detection technique. Imaging Sci J [Internet]. 2018 May 19 [cited 2019 Jan 30];66(4):254–62. Available from: https://www.tandfonline.com/doi/full/10.1080/13682199.2017.1420021
8. Pun C-M, Chung J-L. A two-stage localization for copy-move forgery detection. Inf Sci (Ny) [Internet]. 2018 Oct 1 [cited 2019 Apr 28];463–464:33–55. Available from: https://www.sciencedirect.com/science/article/pii/S0020025518304808?via%3Dihub

9. Khayeat ARH, Rosin PL, Sun X. Copy-Move Forgery Detection Using the Segment Gradient Orientation Histogram. In Springer, Cham; 2017 [cited 2019 Apr 28]. p. 209–20. Available from: http://link.springer.com/10.1007/978-3-319-59126-1_18

10. Subrahmanyeswara Rao B. A fuzzy fusion approach for modified contrast enhancement based image forensics against attacks. Multimed Tools Appl [Internet]. 2018 Mar 1 [cited 2019 Jan 30];77(5):5241–61. Available from: http://link.springer.com/10.1007/s11042-017-4426-2

11. Fan J, Cao H, Kot AC. Estimating EXIF Parameters Based on Noise Features for Image Manipulation Detection. IEEE Trans Inf Forensics Secur [Internet]. 2013 Apr [cited 2019 Jan 30];8(4):608–18. Available from: http://ieeexplore.ieee.org/document/6471213/

12. Tralic D, Zupancic I, Grgic S, Grgic M. CoMoFoD - New Database for Copy-Move Forgery Detection. In: Proceedings of 55th International Symposium ELMAR-2013. 2013. p. 49–54.

13. Rassem TH, Khoo BE. Completed local ternary pattern for rotation invariant texture classification. Sci World J. 2014;2014.

14. Hossain MM. Proposed Mean (Robust) in the Presence of Outlier. J Stat Appl Probab Lett. 2016;3(3):103–7.

15. Farid H. Exposing Digital Forgeries in Scientific Images. 2006;

16. Lu W, Sun W, Huang J, Lu H. Digital image forensics using statistical features and neural network classifier. Mach Learn Cybern 2008 Int Conf IEE [Internet]. 2008;5(July):12–5. Available from: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4620890

17. Birajdar GK, Mankar VH. Digital image forgery detection using passive techniques: A survey. Digit Investig [Internet]. 2013;10(3):226–45. Available from: http://dx.doi.org/10.1016/j.diin.2013.04.007

18. Hasoon Khayeat AR. COPY-MOVE FORGERY DETECTION IN DIGITAL IMAGES. 2017.

19. Thajeel SA-N, Sulong G. State of the Art of Copy-Move Forgery Detection Techniques : a Review. Int J Comput Sci Issues (IJCSI. 2013;10(6):174–83.

20. Dixit A, Gupta RK. Copy-Move Image Forgery Detection a Review. Int J Image, Graph Signal Process [Internet]. 2016;8(6):29–40. Available from: http://www.mecs-press.org/ijigsp/ijigsp-v8-n6/v8n6-4.html

21. Dixit A, Dixit R, Gupta RK. DCT and DWT Based Methods for Detecting Copy-Move Image Forgery: A Review. Int J Signal Process Image Process Pattern Recognit. 2016;9(10):249–58.

22. Thajeel SA, Sulong G. A Novel Approach for Detection of Copy Move Forgery using Completed Robust Local Binary. J Inf Hiding Multimed Signal Process. 2015;6(2):351–64.

23. Hashem FS, Sulong G. Passive aproaches for detecting image tampering: A review. J Teknol. 2015;73(2):31–6.

24. Qureshi MA, Deriche M. A Fast No Reference Image Quality Assessment using Laws Texture Moments. 2014;979–83.

25. Puri M, Chopra V. A Survey : Copy-Move Forgery Detection Methods. Int J Comput Syst. 2016;03(09):582–6.

26. Popescu AC, Farid H. Exposing Digital Forgeries by Detecting Duplicated Image Regions [Internet]. 2015 [cited 2018 Aug 13]. Available from: http://www.ists.dartmouth.edu/library/102.pdf

27. Yao H, Wang S, Zhao Y, Zhang X. Detecting Image Forgery Using Perspective Constraints. Signal Processing. 2012;19(3):123–6.

28. Ali Qureshi M, Deriche M. A review on copy move image forgery detection techniques. 2014 IEEE 11th Int Multi-Conference Syst Signals Devices, SSD 2014. 2014;1–5.

29. Kaur S, Julka N. International Journal of Advance Engineering and Research A 2D-DWT Based Enhanced Technique of Copy Move Forgery Detection. 2016;119–23.

30. Pandey RC, Singh SK, Shukla KK. Passive forensics in image and video using noise features: A review. Digit Investig [Internet]. 2016;19(182):1–28. Available from: http://dx.doi.org/10.1016/j.diin.2016.08.002

31. Rajath B, Sunitha K. Survey on Passive Image Tampering Detection. 2016;3(4).

32. Singh R, Kaur M. Copy move tampering detection techniques: A review. Int J Appl Eng Res. 2016;11(5):3610–5.

33. Park C-S, Kim C, Lee J, Kwon G-R. Rotation and scale invariant upsampled log-polar fourier descriptor for copy-move forgery detection. Multimed Tools Appl [Internet]. 2016 Dec 11 [cited 2019 Apr 28];75(23):16577–95. Available from: http://link.springer.com/10.1007/s11042-016-3575-z

34. Mao Q, Chang CC, Harn L, Chang SC. An image-based key agreement protocol using the morphing technique. Multimed Tools Appl. 2015;74(9):3207–29.

35. Bagade AM, Talbar SN. A High Quality Steganographic Method Using Morphing. 2014;10(2).

36. Zandi M, Mahmoudi-Aznaveh A, Talebpour A. Iterative Copy-Move Forgery Detection Based on a New Interest Point Detector. IEEE Trans Inf Forensics Secur. 2016;11(11):2499–512.

37. Pan X, Lyu S. Region duplication detection using image feature matching. IEEE Trans Inf Forensics Secur. 2010;5(4):857–67.

38. Dixit A, Gupta RK. A Hybrid Method for Copy-Move Forgery Detection Based on Wavelet Transform and Texture Analysis. Int J Emerg Res Manag &Technology. 2016;5(5):32–7.

39. Park C-S, Kim C, Lee J, Kwon G-R. Rotation and scale invariant upsampled log-polar fourier descriptor for copy-move forgery detection. Multimed Tools Appl [Internet]. 2016;1–19. Available from: http://link.springer.com/10.1007/s11042-016-3575-z

40. Zheng L, Zhang Y, Thing VLL. A survey on image tampering and its detection in real-world photos. J Vis Commun Image Represent [Internet]. 2019 Jan 1 [cited 2019 Apr 29];58:380–99. Available from: https://www.sciencedirect.com/science/article/pii/S104732031830350X?via%3Dihub

41. Tralic D, Zupancic I, Grgic S, Grgic M. CoMoFoD - New Database for Copy-Move Forgery Detection. Proc 55th Int Symp ELMAR-2013. 2013;(September):25–7.

42. Lowe DG. Object recognition from local scale-invariant features. In: Proceedings of the Seventh IEEE International Conference on Computer Vision [Internet]. IEEE; 1999 [cited 2019 Jan 30]. p. 1150–7 vol.2. Available from: http://ieeexplore.ieee.org/document/790410/

43. Xu B, Wang J, Liu G, Dai Y. Image copy-move forgery detection based on SURF. Proc - 2010 2nd Int Conf Multimed Inf Netw Secur MINES 2010. 2010;889–92.

44. Bay H, Ess A, Tuytelaars T, Van Gool L. Speeded-Up Robust Features (SURF). Comput Vis Image Underst [Internet]. 2008 Jun 1 [cited 2019 Jan

30];110(3):346–59. Available from: https://www.sciencedirect.com/science/article/pii/S1077314207001555

45. Zandi M, Mahmoudi-Aznaveh A, Talebpour A. Iterative Copy-Move Forgery Detection Based on a New Interest Point Detector. IEEE Trans Inf Forensics Secur [Internet]. 2016;6013(c):1–1. Available from: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7500083

46. Wenchang S, Fei Z, Bo Q, Bin L. Improving image copy-move forgery detection with particle swarm optimization techniques. China Commun [Internet]. 2016 Jan [cited 2019 Jan 30];13(1):139–49. Available from: http://ieeexplore.ieee.org/document/7405711/

47. Soni B, Das PK, Thounaojam DM. multiCMFD: fast and efficient system for multiple copy- move forgeries detection in image. In: ACM International Conference Proceeding Series. 2018. p. 53–8.

48. Zhao Y, Jia W, Hu R-X, Min H. Completed robust local binary pattern for texture classification. Neurocomputing. 2013;106:68–76.

49. Mahdian B, Saic S. Detection of copy-move forgery using a method based on blur moment invariants. Forensic Sci Int. 2007;171(2–3):180–9.

50. Kashyap A, Joshi SD. Detection of copy-move forgery using wavelet decomposition. 2013 Int Conf Signal Process Commun ICSC 2013. 2013;396–400.

51. Le Z, Xu W. A robust image copy-move forgery detection based on mixed moments. Proc IEEE Int Conf Softw Eng Serv Sci ICSESS. 2013;(208098):381–4.

52. Wang X yang, Liu Y nan, Xu H, Wang P, Yang H ying. Robust copy–move forgery detection using quaternion exponent moments. Pattern Anal Appl. 2018;21(2):451–67.

53. Sunil K, Jagan D, Shaktidev M. DCT-PCA Based Method for Copy-Move Forgery Detection. In: ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of CSI - Volume 2 [Internet]. 2014. p. 577–83. Available from: http://link.springer.com/10.1007/978-3-319-03095-1

54. Li K, Li H, Yang B, Meng Q, Luo S. Detection of Image Forgery Based on Improved PCA-SIFT. In: Computer Engineering and Networking, Lecture Notes in Electrical Engineering 277. 2014. p. 679–86.

55. Zhao J, Guo J. Passive forensics for copy-move image forgery using a method

based on DCT and SVD. Forensic Sci Int. 2013;233(1):158–66.

56. Liu F, Feng H. An efficient algorithm for image copy-move forgery detection based on DWT and SVD. Int J Secur its Appl. 2014;8(5):377–90.

57. Sanap VK, Mane VM. Region duplication forgery detection in digital images using 2D-DWT and SVD. Proc 2015 Int Conf Appl Theor Comput Commun Technol iCATccT 2015. 2015;599–604.

58. Patra SK, Bijwe AD. Copy-Move Image Forgery Detection using SVD. 2016;2220–4.

59. Dixit R, Naskar R, Mishra S. Blur-invariant copy-move forgery detection technique with improved detection accuracy utilising SWT-SVD. IET Image Process [Internet]. 2017;11(5):301–9. Available from: http://digital-library.theiet.org/content/journals/10.1049/iet-ipr.2016.0537

60. Langille A, Minglun Gong. An Efficient Match-based Duplication Detection Algorithm. In: The 3rd Canadian Conference on Computer and Robot Vision (CRV’06) [Internet]. IEEE; [cited 2019 Jan 30]. p. 64–64. Available from: http://ieeexplore.ieee.org/document/1640419/

61. Zimba M, Xingming S. Fast and Robust Image Cloning Detection using Block Characteristics of DWT Coefficients. Int J Digit Content Technol its Appl [Internet]. 2011;5(7):359–67. Available from: http://www.aicit.org/jdcta/paper_detail.html?q=600

62. Davarzani R, Yaghmaie K, Mozaffari S, Tapak M. Copy-move forgery detection using multiresolution local binary patterns. Forensic Sci Int [Internet]. 2013;231(1–3):61–72. Available from: http://dx.doi.org/10.1016/j.forsciint.2013.04.023

63. Zheng N, Wang Y, Xu M. A LBP-Based Method for Detecting Copy-Move Forgery with Rotation. In: Lecture Notes in Electrical Engineering (LNEE). 2013. p. pp 261-267.

64. Brajic M. Overlapping Block Based Algorithm for Copy-Move Forgery Detection in Digital Images. 2016;1:191–8.

65. Santony J, Na`am J. Infiltrate Object Extraction in X-ray Image by Using Math-Morphology Method and Feature Region Analysis. Int J Adv Sci Eng Inf Technol [Internet]. 2016 Feb 29 [cited 2019 Mar 18];6(2):239. Available from: http://ijaseit.insightsociety.org/index.php?option=com_content&view=article

&id=9&Itemid=1&article_id=763

66. Yuhandri -, Madenda S, Wibowo EP, Karmilasari -. Object Feature Extraction of Songket Image Using Chain Code Algorithm. Int J Adv Sci Eng Inf Technol [Internet]. 2017 Feb 25 [cited 2019 Mar 18];7(1):235. Available from: http://ijaseit.insightsociety.org/index.php?option=com_content&view=article&id=9&Itemid=1&article_id=1479

67. Arshad H, Lam MC, Obeidy WK, Tan SY. An Efficient Cloud based Image Target Recognition SDK for Mobile Applications. Int J Adv Sci Eng Inf Technol [Internet]. 2017 Apr 16 [cited 2019 Mar 18];7(2):496. Available from: http://ijaseit.insightsociety.org/index.php?option=com_content&view=article&id=9&Itemid=1&article_id=1744

68. Ojala T, Pietikäinen M, Mäenpää T. Multiresolution Gray Scale and Rotation Invariant Texture Classification with Local Binary Patterns. 2002 [cited 2017 Jan 4]; Available from: http://www.ee.oulu.fi/research/imag/texture

69. Li L, Li S, Zhu H, Chu S-C, Roddick JF, Pan J-S. An efficient scheme for detecting copy-move forged images by local binary patterns. J Inf Hiding Multimed Signal Process. 2013;4(1):46–56.

70. Tan X, Triggs B. Enhanced Local Texture Feature Sets for Face Recognition Under Difficult Lighting Conditions. 2007;168–82.

71. Tan X, Triggs B. Enhanced local texture feature sets for face recognition under difficult lighting conditions. IEEE Trans Image Process. 2010;19(6):1635–50.

72. Rassem TH, Khoo BE. Completed local ternary pattern for rotation invariant texture classification. ScientificWorldJournal [Internet]. 2014 [cited 2017 Jan 4];2014:373254. Available from: http://www.ncbi.nlm.nih.gov/pubmed/24977193

73. Liao S, Law MWK, Chung ACS. Dominant Local Binary Patterns for Texture Classification. IEEE Trans Image Process [Internet]. 2009 May [cited 2017 Jan 4];18(5):1107–18. Available from: http://ieeexplore.ieee.org/document/4808422/

74. Zhenhua Guo, Lei Zhang, Zhang D. A Completed Modeling of Local Binary Pattern Operator for Texture Classification. IEEE Trans Image Process

[Internet]. 2010 Jun [cited 2017 Jan 4];19(6):1657–63. Available from: http://ieeexplore.ieee.org/document/5427137/

75. Zhao G, Wu G, Liu Y, Chen J. Texture Classification Based on Completed Modeling of Local Binary Pattern. 2011 Int Conf Comput Inf Sci [Internet]. 2011;268–71. Available from: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6086187

76. Yuan JH, Huang DS, Zhu HD, Gan Y. Completed hybrid local binary pattern for texture classification. Proc Int Jt Conf Neural Networks. 2014;2050–7.

77. Mohamed AA, Yampolskiy R V. Adaptive extended local ternary pattern (AELTP) for recognizing avatar faces. Proc - 2012 11th Int Conf Mach Learn Appl ICMLA 2012. 2012;1:57–62.

78. Kaushik R, Kumar R, Mathew J. On Image Forgery Detection Using Two Dimensional Discrete Cosine Transform and Statistical Moments. 2015;70:130–6.

79. Mushtaq S, Mir AH. Forgery Detection Using Statistical Features. 2014;(November):92–7.

80. Mukherjee P, Mitra S. International Journal of Computer Science and Mobile Computing A Review on Copy-Move Forgery Detection Techniques Based on DCT and DWT [Internet]. Vol. 4, International Journal of Computer Science and Mobile Computing. 2015 [cited 2019 Jan 30]. Available from: www.ijcsmc.com

81. Yadav N, Kapdi R, Ieee. Copy Move Forgery Detection using SIFT and GMM. 2015 5th Nirma Univ Int Conf Eng. 2015;

82. Christlein V, Riess C, Angelopoulou E. A Study on Features for the Detection of Copy-Move Forgeries. Sicherheit 2010, Gesellschaft für Inform e V. 2010;105–16.

83. Lee J, Chang C, Chen W. Detection of copy – move image forgery using histogram of orientated gradients. Inf Sci (Ny) [Internet]. 2015;321:250–62. Available from: http://dx.doi.org/10.1016/j.ins.2015.03.009

84. Pun CM, Chung JL. A two-stage localization for copy-move forgery detection. Inf Sci (Ny) [Internet]. 2018;463–464:33–55. Available from: https://doi.org/10.1016/j.ins.2018.06.040

85. Zhao X, Li J, Li S, Wang S. Detecting digital image splicing in chroma spaces. Lect Notes Comput Sci (including Subser Lect Notes Artif Intell Lect

Notes Bioinformatics). 2011;6526 LNCS:12–22.

86. Wang Y, Gurule K, Wise J, Zheng J. Wavelet based region duplication forgery detection. Proc 9th Int Conf Inf Technol ITNG 2012. 2012;30–5.

87. Alkawaz MH, Sulong G, Saba T, Rehman A. Detection of copy-move image forgery based on discrete cosine transform. Neural Comput Appl. 2016;30(1):1–10.

88. Hsu CM, Lee JC, Chen WK. An efficient detection algorithm for copy-move forgery. In: Proceedings - 2015 10th Asia Joint Conference on Information Security, AsiaJCIS 2015. 2015. p. 33–6.

89. Dong J, Wang W, Tan T. CASIA image tampering detection evaluation database. 2013 IEEE China Summit Int Conf Signal Inf Process ChinaSIP 2013 - Proc. 2013;422–6.

90. Zampoglou M, Papadopoulos S, Kompatsiaris Y. Detecting image splicing in the wild (WEB). In: 2015 IEEE International Conference on Multimedia & Expo Workshops (ICMEW) [Internet]. IEEE; 2015 [cited 2019 Aug 17]. p. 1–6. Available from: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7169839

91. Wang X, Jiao L, Wang X, Yang H, Niu P. Copy-move forgery detection based on compact color content descriptor and Delaunay triangle matching. Multimed Tools Appl [Internet]. 2019 Jan 7 [cited 2019 Apr 29];78(2):2311–44. Available from: http://link.springer.com/10.1007/s11042-018-6354-1

# APPENDIX A

## Data Description of Copy-Move Forgery Distorted by Post-Processing Attacks

All the tampered images in the database manipulated using different categories of following attacks which are translation, rotation, scaling, and distortion, except shearing attack which are highly useful for the CMFD algorithms evaluation. Additionally, the ground truth for each image is also provided.