Notice of the Final Oral Examination
for the Degree of Doctor of Philosophy

of

BELAL AHMED

MSc (University of Northern British Columbia, 2014)
BSc (Ain Shams University, 2007)

“Detection and Localization of Forgeries in Digital Images”

Department of Electrical and Computer Engineering

Tuesday, December 8, 2020
12:00 P.M.
Remote Defence

Supervisory Committee:
Dr. Aaron Gulliver, Department of Electrical and Computer Engineering, University of Victoria (Supervisor)
Dr. Wu-Sheng Lu, Department of Electrical and Computer Engineering, UVic (Member)
Dr. Saif al Zahir, Department of Computer Science and Engineering, University of Alaska (Outside Member)

External Examiner:
Dr. Kenrick J. Mock, Department of Computer Science, University of Alaska Anchorage

Chair of Oral Examination:
Dr. Maycira Costa, Department of Geography, UVic

Dr. David Capson, Dean, Faculty of Graduate Studies
Abstract

Digital images have become a dominant source of information and means of communication in our society. However, these images can easily be altered using readily available image editing tools. Image tempering can be done in several ways such as image splicing, retouching, and copy-move forgeries.

In copy-move forgery, part of an image is copied and pasted into a different part of the same image for the purpose of hiding or adding an object to the image. In image splicing, part of an image is copied and pasted into a different image. To detect image forgery, image features must first be extracted. A feature is information related to edges, objects or a specific region in the image. In this research, new methods for detecting copy-move forgery and image splicing are introduced. Most existing block-based forgery detection methods use large feature dimensions up to 64 per image block so the complexity is high. However, reducing the feature dimensions lowers the detection accuracy. This research presents a new method of detecting copy-move forgery in images using only 4 features per image block. This method uses steerable pyramid and singular value decomposition (SVD) techniques to decompose and extract features from image blocks. Then the features are sorted lexicographically and matched using the Kolmogorov-Smirnov (KS) test. The proposed algorithm is compared to several well-known techniques and shown to provide better accuracy.

To detect image splicing, a new deep learning method is introduced. This method employs Mask-RCNN to generate masks for spliced regions in forged images. It is specifically designed to learn discriminative artifacts from tampered regions. In this method, a ResNet backbone is used to convert the input image into a feature map. The ResNet-50 and ResNet-101 backbones are considered.

Several techniques have been introduced for image forgery detection. However, most of these techniques only focus on detecting a certain kind of forgery and perform poorly in other cases. As a result, detecting multiple kinds of forgery using one technique remains a problem. In this study, we introduce a novel deep neural architecture specifically designed to detect multiple kinds of forgery, named PADNET.
Unlike other solutions, PADNET is an end-to-end trainable deep neural network which employs feature pyramid network (FPN) to aggregate features from multiscale levels of a ResNet-50 backbone. The feature maps are then used to train a DeepUNet architecture designed to learn discriminative features by considering both high level global features and low-level local features. The convergence of PADNET is tested using two loss functions, binary cross-entropy and weighted binary cross-entropy. Experimental results show that weighted binary cross-entropy is more efficient as a loss function for copy-move forgery while binary cross-entropy is more efficient for image splicing. In addition, the performance of PADNET with training on only the boundaries of the forged area is compared to the network trained on the entire forged area. Evaluation is done using the well known CoMoFoD data set for copy-move forgery and CASIA1 for image splicing forgery. The results obtained demonstrate that PADNET outperforms state-of-the-art copy-move and image splicing forgery detection algorithms.