Table of content

Certificate ... **iii**

Declaration by the Candidate ... **v**

Copyright Transfer Certificate ... **vii**

Acknowledgement ... **ix**

Abstract ... **xi**

Table of content ... **xv**

List of Figures ... **xix**

List of Tables ... **xxv**

List of Symbols ... **xxix**

List of Abbreviations ... **xxxi**

Chapter 1 Introduction ... **1**

1.1 Background ... 1

1.2 Digital Image Forgery ... 2

1.2.1 Types of Digital Image Forgery ... 4

1.2.1.1 Copy Move Forgery ... 4

1.2.1.2 Image Splicing ... 5

1.2.2 Need of the Digital Image Forgery Detection ... 5

1.2.3 Digital Image Forgery Detection Techniques ... 6

1.2.3.1 Active Protection Schemes ... 7

1.2.3.2 Passive Detection Techniques ... 7

1.2.4 Image Authentication Challenges ... 8

1.3 Problem Statement ... 10

1.4 Motivation of the Research ... 10

1.5 Objectives of the Research ... 11

1.6 Contributions to the Thesis ... 12

1.7 Thesis Organization ... 14

Chapter 2 Theoretical Background and Literature Review ... **17**

2.1 Literature review on Copy-Move Forgery Detection ... 18

2.1.1 Block-based Approaches ... 18

2.1.2 Key-point-based Approaches ... 20

2.1.3 Data-driven Approaches ... 21

2.1.4 Research Gaps and Findings ... 21

2.2 Literature review on Spliced Image Detection ... 23

2.2.1 Data-driven Techniques 23
2.2.2 Statistical Techniques 27
2.2.3 Research Gaps and Findings 29
2.3 Dataset Used for Experimental Study 31
2.3.1 CoMoFoD 31
2.3.2 CMFD 32
2.3.3 CASIA v1.0 and CASIA v2.0 33
2.3.4 IEEE IFS Dataset 34
2.3.5 Columbia Uncompressed Dataset (CUD) 35
2.4 Evaluation Metrics 35

Chapter 3 Copy Move Forgery Detection using Statistical and Data-driven Techniques 39

3.1 Background 39
3.2 Research Gaps 41
3.3 Proposed Models 42
3.3.1 Copy-Move Image Forgery Detection using DCT and ORB Feature Set 42
3.3.1.1 Method and Model 43
3.3.1.2 Result Analysis and Discussion 48
3.3.2 Detection of copy-move forgery in digital image using a multi-scale, multi-stage deep learning model 51
3.3.2.1 Method and Model 52
3.3.2.2 Result Analysis and Discussion 59
3.4 Summary 69

Chapter 4 Spliced Image Forgery Detection using Intrinsic Footprints of an Image 71

4.1 Background 71
4.2 Research Gaps 73
4.3 Proposed Method 74
4.3.1 A Technique for Image Splicing Detection using Hybrid Feature Seet 74
4.3.1.1 Method and Model 74
4.3.1.2 Result Analysis and Discussion 83
4.3.2 Spliced image forgery detection and localization using inconsistent noise pattern 89
4.3.2.1 Proposed Inconsistent Noise Pattern Estimation Technique 90
4.3.2.2 Method and Model 94
4.3.2.3 Result Analysis and Discussion 100
4.4 Summary 110

Chapter 5 Data-driven techniques for detection and localization of blind image forgery 113

5.1 Background 114
5.2 Research Gaps 116
5.3 Proposed Methods 119

5.3.1 Modified U-Net Model for Detection of Forged Region in Images Acquired from Variant Sources 119
5.3.1.1 Existing Model 120
5.3.1.2 The Proposed Modified Architecture 122
5.3.1.3 Experimental Analysis and Discussion 126
5.3.2 An investigation and analysis of forged digital document using deep inception network 135
5.3.2.1 The Proposed Dataset 136
5.3.2.2 The Proposed Model 139
5.3.2.3 Result Analysis and Discussion 145
5.4 Summary 157

Chapter 6 Conclusion and Future Directions 159
6.1 Conclusion 159
6.2 Future Research Directions 163

List of Publications 172

References 174

List of Figures

Figure 1.1: Example of editing of an image with mild processing (a) Original Lenna Image (b) Color processed Lenna image (c) Image with noise addition 3

Figure 1.2: Examples of digital image forgery (region alteration) (a) Original Image (b) Image Splicing (c) Original Image (d) Copy-move forgery 4

Figure 1.3: Outline of the thesis..... 14

Figure 2.1: An Image acquisition pipeline..... 18

Figure 2.2: Steps involved in Block-Based CMFD Techniques..... 18

Figure 2.3: Steps involved in Keypoint Matching Based CMFD Techniques 20

Figure 2.4: Steps involved in Keypoint Matching Based CMFD Techniques 21

Figure 2.5: The instances of the CoMoFoD dataset 31

Figure 2.6: The instances of the CMFD dataset 33

Figure 2.7: Demonstration of IEEE IFS Dataset 35

Figure 2.8: Visualization of Columbia Uncompressed Dataset..... 35

Figure 3.1: Examples of Copy Move Forgery (CoMoFoD dataset [68]) (a) Original Image (b) Forged Image (c) Ground Truth mask of Forged Image..... 40

Figure 3.2: The framework of the proposed CMFD technique 43

Figure 3.3: The order in which a block's features are extracted. Coefficients on the diagonal have the same frequency 44

Figure 3.4: (a)The red dot depicts the pixel under consideration. The surrounding pixels values that correspond to its feature are depicted with a red border. (b)The extracted feature vector of length 16 [75] 45

Figure 3.5: Image [a1-a6]: Forged Images where a1: Copy-move, a2: multiple copy-move, a3: copy-rotate-move, a4: copy-scale-move, a5: copy-scale-move, a6: combination

of all; [b1-b6]: Ground truth images related to [a1-a6]; and [c1-c6]: Results of the proposed methods.....49
Figure 3.6: (a) to (e) depicts the comparison charts for various levels of post-processing operations and the respective number of images passed by the techniques.....51
Figure 3.7: Visual Representation of Multi-Scale Network.....52
Figure 3.8: Block-Diagram of the Proposed Model.....53
Figure 3.9: An Illustration of max-pooling of activated feature space and then the concatenation of another level feature space with first level feature space 54
Figure 3.10: Architecture of proposed model for copy-move forgery detection using deep learning CNN model 55
Figure 3.11: Accuracy and Loss of model (3x3) during training on CMFD dataset 58
Figure 3.12: Accuracy and Loss of model (3x3) during training on CoMoFoD dataset 58
Figure 3.13: Visual result of the proposed model on test images of CoMoFoD dataset 61
Figure 3.14: Performance analysis of the proposed model using line graph on CoMoFoD dataset (a) Precision, recall, accuracy and F1-score (b) TNR and MCC values 62
Figure 3.15: The visual results of the proposed model on images of the CMFD Dataset 66
Figure 3.16: Performance analysis of the proposed model using line graph on CMFD dataset (a) **p**recision, **r**ecall, **a**ccuracy and **F1**-score (b) TNR and MCC values 67
Figure 3.17: Image level analysis of the proposed model on datasets (a) CoMoFoD (b) CMFD.....68
Figure 4.1: Examples of Spliced Image Forgery (a) First Original Image (b) Second Original Image (c) Spliced Image (Combination of both) 72
Figure 4.2: Flow Diagram of the Proposed method.....75
Figure 4.3: Color Conversion of the input image.....75

Figure 4.4: Multiple features from the input image Gray-level color space..... 76

Figure 4.5: Extraction of HoG Based Features from Pre-processed Image..... 77

Figure 4.6: Extraction of LTE Based Features from Pre-processed Image 79

Figure 4.7: Frequency Representation of DWT..... 79

Figure 4.8: Extraction of DWT Based Features from Pre-processed Image 80

Figure 4.9: Extraction of LBP Features from Pre-processed Image..... 81

Figure 4.10: Overall Framework for Image Forgery Detection..... 83

Figure 4.11: Result Analysis of the Proposed method on CASIA v1.0 dataset 84

Figure 4.12: Result Analysis of Proposed method on CASIA v2.0 dataset 86

Figure 4.13: Result Analysis of Proposed method on COLUMBIA dataset 87

Figure 4.14: A Failure Case of the Proposed System 89

Figure 4.15: Graphical Abstract Representation of Proposed Approach (Overall method of spliced image detection and localization)..... 95

Figure 4.16: The Pre-processed result of Input Image (Conversion of a color image into Grayscale) 96

Figure 4.17: Result of Wavelet Transformed Image (Approximation and Detail Coefficients)..... 96

Figure 4.18: Noise Statistic Estimation of Diagonal Component of Discrete Wavelet Transformed Image..... 98

Figure 4.19: Result after post-processing (After Morphological Operations)..... 100

Figure 4.20: Result of Image Splicing detection and localization on Columbia uncompressed dataset (a) Test Image (b) Ground Truth Mask (c) Localized splice region result of BLNVS [13] (d) Localized splice region result of PKNV [14] (e) Localized splice region result of NIBIF [16] (f) Noise Statistic Map of the given method (g)

Localized Spliced Region from the Noise Map (h) Color Overlay of the spliced region on the RGB input Image.....101
Figure 4.21: Result of Image Splicing detection and localization on CAISA and IEEE IFS-TC Image forensics Challenge datasets (a) Test Image (b) Ground Truth Mask (c) Localized splice region result of BLNVS [13] (d) Localized splice region result of PKNV [14] (e) Localized splice region result of NIBIF [16] (f) Noise Statistic Map of the given method (g) Localized Spliced Region from the Noise Map (h) Color Overlay of the spliced region on the RGB input Image.....106
Figure 4.22: Proof of the proposed algorithm on authentic images of datasets (a) Natural Color Image (b) Noise Mapped Image (c) Localized Spliced Region.....108
Figure 4.23: (a) Comparison of the Accuracy value of the proposed work with other techniques (b) Comparison of Matthews Correlation Coefficient value of the proposed work with other techniques.....109
Figure 4.24: (a) Comparison of F1-Score value of proposed work with other techniques (b) Comparison of Elapsed Time of proposed work with other techniques.....110
Figure 5.1: Example of forgery in a digital document (a) Original Image (b) Forged Image and the forged region is shown in a red box (c) Ground Truth of forged Image.....115
Figure 5.2: Architecture of the Identity Block.....123
Figure 5.3: Architecture of the proposed model for localization of manipulated regions in Forged Image.....125
Figure 5.4: Training Result of the proposed model (a) Accuracy (b) Loss on Different Epochs.....128
Figure 5.5: Visual Results on a different image of Dataset (a) Forged Color Image (b) Ground Truth Mask (c) Result by the proposed model (d) Result by U-Net model (e) Result by Encoder-Decoder Model.....129

Figure 5.6: Visual Results of the proposed methods on different test cases acquired from different sources 131
Figure 5.7: Comparison of the proposed method with state-of-the-arts techniques for Image Forgery Detection 134
Figure 5.8: Tree structure of directory and content of the constructed dataset 137
Figure 5.9: Inception Block without Dimension Reduction used in Proposed Architecture 140
Figure 5.10: Architecture of the proposed model for forged document detection 142
Figure 5.11: Training result of the proposed model on FD3 dataset 144
Figure 5.12: Confusion matrix and corresponding heat map of Image-Level analysis of the proposed and compared models on test cases of FD3 dataset 146
Figure 5.13: The visual result of the test data from the publicly available data (a) Tampered document (b) Ground Truth Mask (c) Result given by the proposed model (d) Result given by U-net (e) Result given by Linknet 148
Figure 5.14: The visual result of the copy-move forgery test data from the constructed dataset FD3 (a) Tampered document (b) Ground Truth Mask (c) Result given by the proposed model (d) Result given by U-net (e) Result given by Linknet 149
Figure 5.15: The compared average result (accuracy, F1-score, and MCC value) of the proposed model with other state-of-the-arts on individual operations of copy-move forged documents 151
Figure 5.16: The visual result of the spliced test data from the constructed dataset FD3 (a) Tampered document (b) Ground Truth Mask (c) Result given by the proposed model (d) Result given by U-net (e) Result given by Linknet 152

Figure 5.17: The compared average result (accuracy, F1-score and MCC value) of the proposed model with other state-of-the-arts on individual operations of spliced forged documents.....154
Figure 5.18: Visual demonstration of misclassified results by the proposed method...156