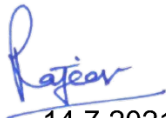


Certificate

It is certified that the work contained in the thesis titled “*DESIGN AND DEVELOPMENT OF SOME APPROACHES FOR DIGITAL IMAGE FORGERY DETECTION AND LOCALIZATION*” by **Ankit Kumar Jaiswal** has been carried out under my supervision and that this work has not been submitted elsewhere for a degree.

It is further certified that the student has fulfilled all the requirements of Comprehensive, Candidacy and State-of-the-art seminar.



14.7.2021

Signature of Supervisor

Prof. Rajeev Srivastava

Department of Computer Science and Engineering

Indian Institute of Technology (BHU), Varanasi

Declaration by the Candidate

Copyright Transfer Certificate

Title of the Thesis: Design and development of some approaches for digital image forgery detection and localization

Name of the Student: Ankit Kumar Jaiswal

Copyright Transfer

The undersigned hereby assigns to the Indian Institute of Technology (Banaras Hindu University), Varanasi all rights under copyright that may exist in and for the above thesis submitted for the award of the DOCTOR OF PHILOSOPHY.

Date: 14/07/2021

Place: Varanasi

Ankit Jaiswal

Signature of the Student

(Ankit Kumar Jaiswal)

Note: However, the author may reproduce or authorize others to reproduce material extracted verbatim from the thesis or derivative of the thesis for author's personal use provided that the source and the Institute's copyright notice are indicated.

Acknowledgement

I sincerely thank all those people who have helped me to complete this thesis work, directly or indirectly. It is my privilege that I have got an opportunity to thank all those people who have helped me.

First and foremost, I would like to praise and thank **Baba Vishwanath** and **Mata Annapurna**, the almighty, who has granted countless blessing and knowledge so that I have been finally able to accomplish this thesis. My millions of salutes go to **Mahamana Pandit Madan Mohan Malviya ji**, the founder of Banaras Hindu University, Varanasi for his service to humanity, great vision and creation of this glorious institute.

I want to express my heartfelt gratitude to my supervisor **Prof. Rajeev Srivastava**, who has not only directly helped me in my PhD work, but at every turn in this period of life. His advice, encouragement and critics are the sources of innovative ideas, inspiration is the causes behind the successful completion of this. Thesis work. The confidence shown on me by him was the biggest source of inspiration for me. It has been a privilege working with him for several years.

I would like to express my deepest appreciation to my research progress evaluation committee members Prof. K. K. Shukla of the Department of Computer Science and Engineering and Prof. T. Som, Department of Mathematical Sciences IIT (BHU), for providing continuous support, encouragement, and advice. I'd like to thank Dr. Prateek Chattopadhyay, Assistant Professor for his suggestions and comments.

I'm extremely grateful to all the professors, deans, office staff, supporting staff and PhD Research Scholars of Indian Institute of Technology (BHU) Varanasi India. I express

my gratitude to the Director, Registrars, Deans, Heads, and Student Alumni of the Indian Institute of Technology (BHU) Varanasi.

I'd like to extend my gratitude to Dr. Vibhav Prakash Singh (Assistant Professor MNNIT Allahabad), Dr. Jani Kuntesh Ketan (GEC, Gujrat), Dr. Roshan Singh (System Analyst IIT BHU Varanasi), Dr. Gargi Srivastava (Assistant Professor, RGPIT Jais Amethi), Dr. Sarvesh Pandey (Assistant Professor, MMV BHU Varanasi), Dr. Nagendra Pratap Singh (Assistant Professor, NIT Hamirpur) and Dr. Gaurav Baranwal (Assistant Professor, BHU Varanasi). Their insightful comments and constructive criticisms at different stages of my research were thought-provoking and they helped me to focus on my work. I also wish to thank my lab members Santosh Kumar Tripathi, Pratishtha Verma and Divya Singh for their consistent support and help during my research work. I'm thankful to non-teaching staff Mr. Ravi Bharti, Mr. Ritesh Singh, Mr. Shubham Pandey, Mr. Prakhar and Mr. Manoj Kumar Singh, for their support.

It is also necessary to thank those who have neither let my courage down nor left me alone during my PhD duration. I'd like to thank my friends Amit Biswas, Amit Kumar, Nirbhay Kumar Tagore, and Shashank Kumar Singh. Special thanks to Shiksha Singh for her insightful comments, invaluable advice, and unwavering support during my PhD work. I'd also thank Manisha Singh for her constructive criticism and relentless suggestions.

Finally, my family has supported and helped me along the course of this thesis by giving encouragement and providing the moral and emotional support I needed to complete my thesis. To them, I am eternally grateful.

Ankit Kumar Jaiswal

Abstract

In today's image driven world, we heavily rely on digital image data for various purposes – from entertainment to space research. Human brain is naturally accustomed to process visual contents at a greater speed; it is also called as the information currency. With sudden increase in image editing applications, one can easily make alteration in any image. Images shared using smart & mobile devices are hard to trust as an authentic one. It is a challenging task to cope up with ever increasing cases of alteration of images with malicious intentions. Altering the content of an image changes the semantics of the image and treated as digital image forgery. Digital image forgery is categorized into two categories – copy-move forgery and image splicing. Copy-move forgery is performed using a basic photo editing application where a part of an image is copied and pasted onto the same image. Image splicing is a composition technique in which cropped region of an image is pasted onto another image. For confirming the creditability of digital image without their prior knowledge, an image authentication method is required.

A lot of literature has been reported for the detection of forged image based on the intrinsic traces left by different component of digital camera during digital image acquisition process. It could be sensor-based noise inconsistent pattern, color filter array, lighting condition or even the metadata of the image. Due to the sensitive nature towards pixel value alteration such as brightness or contrast adjustment, post processing operations on the forged region is the major challenge in existing detection techniques. Existing copy-move forgery detection techniques suffers from the limitations of geometrical transformation of forged region and computation cost. Similarly, spliced image forgery detection techniques have shortcoming like single scope of application with single footprint, estimation of qualified sensor pattern and non-suitable features for

machine learning classification. Detection of forged scanned document is still an open research issue. These limitations are taken as motivation to navigate a path ahead in the direction of overcoming them. So, key objectives of the research are advancement in existing copy-move and spliced image forgery detection techniques, development of a generalized model for blind forgery detection and development of a model for forged scanned document detection. Thus, the problem statement can be defined as- Design and development of some digital image forgery detection techniques — copy-move, spliced image and forged scanned document centred— to address various challenges with existing image forgery detection methods.

The main work of this thesis is to study and implement existing forgery detection techniques, mentioning their merits and demerits with close analysis and proposing new methods. First, this thesis focuses on a comprehensive literature review on types of image forgery detection methods including types of forgery. Then, a comparative study is done of various copy-move forgery detection techniques (i.e. block-based, keypoint-based and data-driven) by mentioning the pros and cons of the same and some models are then constructed based on the mentioned criteria for copy-move forgery detection. Key-point based techniques are sensitive with post-processing operations such as brightness change or contrast adjustment while block-based approaches are not robust against geometrical transformation. So, a technique is developed using combination of both (keypoint and block-based). Except this, to reduce detection time, a multi-scale multi-stage deep learning model is proposed which is robust against geometrical transformation overcomes the challenges of post-processing operations. The key intention of the research is to cover the existing literature on image splicing detection techniques as well as their comparative study. Non-suited features and non-qualified sensor noise pattern are crucial provocations in image splicing detection techniques. A technique is developed to classify the image

into forged and authentic using combination of handcrafted features and machine learning classifier. To localize the forged region an inconsistent noise pattern-based technique is developed. A qualified noise pattern detects the inconsistent pattern between forged and authentic region of an image. Finally, the major endowment of the thesis is to design some of the efficient data-driven methods which locate the suspected region in an altered image or in a forged digital document whose type of forgery is not known. Due to the different characteristics of digital documents, techniques of digital image forgery detection don't work with forged digital documents. In this case, the most important challenge is the unavailability of publicly available dataset. Thus, a forged digital document dataset is also constructed with the model to detect them.

All the proposed models presented in this thesis are evaluated on multiple publicly available datasets and compared with state-of-the-art techniques. Experimental results of the proposed copy-move forgery detection techniques show that these techniques are not only efficient in detecting copy-move forged regions but also robust towards brightness, contrast change, noise addition, geometric transformations like scaling and rotation and multiple copy-move forgeries. The machine learning-based proposed spliced image forgery detection technique can discriminate the altered images from original images instantly. Whereas inconsistent noise pattern-based spliced image forgery detection technique can locate the forged region in a manipulated image. The developed blind forgery detection technique passed test cases of different synthetic forged images whose acquisition sources are different. Finally, the developed data-driven model for the detection of forged digital documents works on different post-processing operations as well as geometrical transformations of manipulated regions. This thesis also discusses the possible research direction in the area of digital image forgery detection.

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	xxxii
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 Set.....	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

List of Tables

Table 2.1: Related works and their comparison on different parameters	22
Table 2.2: Advantages and Limitations of various state-of-the-art techniques for Image Splicing Detection.....	31
Table 2.3: Details of CoMoFoD dataset	32
Table 2.4: Details of CMFD dataset	33
Table 2.5: Details of CASIA v1.0 and CASIA v2.0 datasets	34
Table 3.1: Performance evaluation on simple copy-move forgery attack on CoMoFoD dataset	50
Table 3.2: Performance comparison. #Passed represents the number of forged images that were successfully detected from a set of 200 forged images.....	50
Table 3.3: Training result of the proposed model on the various kernel size of convolutional layers (i.e. 3x3, 5x5 and 7x7).....	58
Table 3.4: Average test result using performance measures precision, recall, accuracy, TNR, FNR, F1-score and MCC value on different datasets	60
Table 3.5: Average test result using performance measures precision, recall, accuracy, TNR, FNR, F1-score and MCC value on CoMoFoD dataset on different post-processing operations.....	60
Table 3.6: The compared result of the proposed model with state-of-the-art methods on images of CoMoFoD dataset without any post-processing and with JPEG compression quality factor (qf) = 90.....	63
Table 3.7: The compared result of the proposed model with state-of-the-art methods on images of CoMoFoD dataset with Noise addition (variance = 0.0005) and Image Blurring	64

Table 3.8: The compared result of the proposed model with state-of-the-art methods on images of the CoMoFoD dataset with brightness change, color reduction and contrast adjustment	65
Table 3.9: The proposed model result on CMFD dataset on different transformation ...	66
Table 3.10: Image level analysis of the proposed model on different datasets.....	68
Table 4.1: List of features used in the Proposed Approach	81
Table 4.2: Experimental Result of the Proposed method on CASIA v1.0 dataset.....	84
Table 4.3: Experimental Result of the Proposed method on CASIA v2.0 dataset.....	85
Table 4.4: Experimental Result of the Proposed method on COLUMBIA dataset	86
Table 4.5: Running Time, Prediction Speed of different Classifiers on chosen Datasets	88
Table 4.6: Experimental Result of the Proposed method on datasets	88
Table 4.7: Comparison of the proposed algorithm with state-of-the-art techniques on evaluation metrics precision, recall, tnr and accuracy on Columbia Uncompressed dataset	102
Table 4.8: Comparison of the proposed algorithm with state-of-the-art techniques on evaluation metrics elapsed time (in seconds), csi, f1 and mcc on Columbia Uncompressed dataset.....	103
Table 4.9: Average Elapsed Time, precision, recall, tnr, accuracy, csi, f1-score and mcc on Columbia Uncompressed dataset	105
Table 4.10: Comparison of the proposed algorithm with state-of-the-art techniques on evaluation metrics precision, recall, tnr and accuracy on IEEE IFS and CASIA dataset	107

Table 4.11: Comparison of the proposed algorithm with state-of-the-art techniques on evaluation metrics elapsed time (in seconds), csi, f1 and mcc on CASIA and IEEE IFS dataset	107
Table 4.12: Average Elapsed Time, precision, recall, tnr, accuracy, csi, f1-score and mcc on IEEE IFS and CASIA dataset	108
Table 5.1: An overview of existing state-of-art techniques.....	118
Table 5.2: Brief Description of Publicly Available Forged Image Datasets	126
Table 5.3: Average result of the proposed model and other standard models on the available dataset.....	129
Table 5.4: Comparison of Result on Different Evaluation Metrics for Images of Different Publicly Available Dataset.....	130
Table 5.5: Result of Proposed Technique on Different Test Cases	132
Table 5.6: Comparison of Proposed Technique with Similar Techniques of Forged Region Localization	133
Table 5.7: Details of the Constructed Dataset	138
Table 5.8: Training Result of the proposed and other standard models	145
Table 5.9: Image Level Comparison of the Proposed Model with Existing Models....	147
Table 5.10: Comparison of Average result of the proposed model and state-of-the-arts on the publicly available dataset [125]	148
Table 5.11: Comparison of Average result on copy-move forged documents for the proposed and other standard methods.....	149
Table 5.12: Quantitative Result of Copy-Move Forgery Documents on Different Operations for the proposed and other standard models.....	150
Table 5.13: Comparison of Average result of spliced forged documents for the proposed and other standard models	151

Table 5.14: Average Quantitative values of performance measure of Spliced Documents
for the proposed and other standard models..... 153

Table 5.15: Comparison of overall performance on forged document dataset for the
proposed and other standard models 154

Table 5.16: Comparison of time and memory for the proposed and other standard models
..... 155

List of Symbols

I	2-D Image
$f(x,y)$	Intensity at any pair coordinate (x,y)
I_o	Original Image
R_i	i^{th} Region in any image
\emptyset	Empty set or null set
\cup	Union
\cap	Intersection
p	Precision
r	Recall
$f1$	F1-score or F1-measure
s	Specificity
a	Accuracy
m	Miss-rate
mcc	Mathews Correlation coefficient
$/csi$	Critical Success Index
b	Block Size
w, h	Image width and image height in pixels
S_{pc}	State of considered pixel (brightness class)
I_{pc}	The intensity of the considered pixel
T_h	Threshold Value
$I(x,y)$	Intensity of pixel at location (x,y)
$H(P)$	Entropy
c	Number of components in the positive class
\bar{c}	Number of components in the negative class
IM_{rs}	Oriented FAST point
$atan2$	A variant of arc tan
$Sim(x)$	The intensity of the smooth patch of the image
C_T	Count Threshold for shift vector
L	Loss function
w	Weight
$f(x)$	Feature Vector
$stdDev$	Standard Deviation
$h_{\emptyset}(x)$	Hypothesis Function

ϕ	Cost Function
$\psi(x)$	Sigmoid Function
$F_1 \dots F_n$	Extracted Features
I_c	Captured Image by Camera Device
I_l	Ideal image (without noise)
η	Noise present in the image
$\mathcal{E}(I)$ or μ	Expectation or Mean of the image I
var	Variance
κ	Kurtosis
W_ϕ	Approximation Coefficients of wavelet transformed image
W_ψ	Detailed Coefficients of wavelet transformed image
Q_i^j	i^{th} quartile of j^{th} level
v	The binary pattern of the estimated noise
m, n	Height and width of the image (pixels)
SE	Structuring Element for morphological operation
\times	Not Applicable
\checkmark	Applicable
\otimes	Convolution operation
\mathbb{R}^d	Set of Real number of d dimension
μ_B	Mean of batch
σ_B^2	Variance of batch

List of Abbreviations

ANN	Artificial Neural Network
BRIEF	Binary Robust Independent Elementary Features
CAR	Classification alarm rate
CFA	Color Filter Array
CMF	Copy Move Forgery
CMFD	Copy Move Forgery Detection
CNN	Convolutional Neural Network
DCT	Discrete Cosine Transform
DFT	Discrete Fourier Transform
DWT	Discrete Wavelet Transform
ELA	Error Level Analysis
FAR	False alarm rate
FAST	Features from Accelerated Segment Test
FN	False Negative
FNR	False negative rate
FP	False Positive
FPR	False positive rate
GLCM	Grey Level Co-occurrence Matrix
HoG	Histogram of Gradient
IFD	Image Forgery Detection
JPEG	Joint Photographic Expert Group
LBP	Local Binary Pattern
LSTM	Long Short Term Memory
LTE	Laws Texture Energy
MAD	Median absolute deviation
MAR	Miss alarm rate
NLF	Noise level function
NV	Noise Variance
ORB	Oriented FAST and Rotated BRIEF
PCA	Principal Component Analysis
ReLU	Rectified Linear Unit

RGB	Red, Green and Blue Color Space
SD	Standard deviation
SHA	Secure Hash Algorithm
SIFT	Scale Invariant Feature Transform
SURF	Speeded up robust features
SVD	Singular Valued Decomposition
SVM	Support Vector Machine
SWT	Stationary Wavelet Transform
TN	True Negative
TNR	True negative rate
TP	True Positive
TPR	True positive rate
YCbCr	Luminance and Chrominance Color Space