



Developing an Optimal Strategy to Address the Vulnerability of Image Tampering

P. M. I. N Kumara
MS22910172

A THESIS
SUBMITTED TO
SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY
IN PARTIAL FULFILMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
MASTER OF SCIENCE IN INFORMATION TECHNOLOGY
(CYBERSECURITY)

December 2024

I certify that I have read this thesis and that in my opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.

Mr. Kanishka Yapa (Supervisor)

Approved for MSc. Research Project:

MSc. Programme Co-ordinator, SLIIT

Approved for MSc:

Head of Graduate Studies, FoC, SLIIT

DECLARATION

This is to certify that the work is entirely my own and not of any other person, unless explicitly acknowledged (including citation of published and unpublished sources). The work has not previously been submitted in any form to the Sri Lanka Institute of Information Technology or to any other institution for assessment for any other purpose.

Sign:



(P. M. I. N. Kumara)

Date: 22/10/2024

ABSTRACT

Developing an Optimal Strategy to Address the Vulnerability of Image Tampering

P. M Isuranga Nipun Kumara

MSc. in Information Technology specialize in Cybersecurity

Supervisor: Mr. Kanishka Yapa

December 2024

The paper proposes a hybrid image tampering detection system that incorporates the Convolutional Neural Networks into the pool of traditional forensic techniques such as Error Level Analysis and noise analysis. Its objective is to provide high detection accuracy in tampered images through deep learning and forensic methods. According to this method, ELA detects compression inconsistencies in the system, while noise analysis detects abnormal noise patterns in the image. A combination of these techniques provides the capability for the system to capture various methods for tampering, including copy-move forgery, splicing, and subtle retouching. It was trained and tested on the CASIA 2.0 dataset with high accuracy: 98% training accuracy and over 96% validation accuracy. It was successfully deployed as a real-time Flask web application wherein users can upload an image and perform the analysis very quickly. While powerful, the model has a limitation of only revealing a subset of lossless image format tampering and performs subtle manipulations. The future work will involve enhancing scalability and deepfake detection that can handle complex techniques of tampering. The research proposed herein provides a holistic and scalable solution for the detection of image tampering to be applied in digital forensics, verification of media, and cybersecurity.

ACKNOWLEDGEMENT

Without the constant support of my supervisors, Mr. Kanishka Yapa, (Lecturer), Department of Computer Systems Engineering, Sri Lanka Institute of Information Technology, I would not have been able to complete this research. By offering essential comments and helping us through my blunders, He has helped me make the project a success and generate more efficient outcomes. I'd also like to thank panel members for giving us invaluable advice in helping me comprehend the research's flaws and proposing ways to improve the research's functionality.

I'd also like to express my gratitude to coordinators, the course's comprehensive design and analysis lecturer, for giving us the required assistance throughout this project module enabling to address the flaws we encountered effectively. Finally, I'd like to express appreciation to everyone who helped me complete this study, whether directly or indirectly. Your invaluable help and suggestions inspired us to achieve this task.

TABLE OF CONTENTS

DECLARATION	ii
ABSTRACT.....	iii
ACKNOWLEDGEMENT	iv
TABLE OF CONTENTS.....	v
List of Figures	viii
List of Tables	ix
Chapter 1 Introduction	1
1.1 Research Background.....	1
1.1.1 Background of Image Tampering.....	2
1.1.2 Evolution of Image Tampering Detection	2
1.1.3 Unique Contribution of This Research.....	3
1.1.4 Practical Application of the System	4
1.1.5 Practical Applications of this System are in:.....	4
1.2 Literature Review.....	5
1.2.1 Introduction to Image Tampering and Its Implications	5
1.2.2 Traditional Methods of Image Forensic	5
1.2.3 Machine Learning and Deep Learning Approaches in Tampering Detection.....	6
1.2.4 The Hybrid Approach: Forensics-Deep Learning Combination	7
1.2.5 Noise Detection and Laplacian Variance	8
1.2.6 Practical Applications of Image Tampering Detection Systems	8
1.2.7 Challenges in Image Tampering Detection	8
1.2.8 Interpretability and Transparency.....	9
1.2.9 Hybrid Approaches and the Way-Ahead for Tamper Detection	10
1.2.10 Real-World Impact and Applications	10
1.3 Research Problem.....	11
1.4 Research Gap.....	12
1.5 Significant of the Study.....	12
1.6 Research Objectives	13
1.6.1 The Main Objective	13
1.6.2 Sub Objectives.....	13
1.7 Organization of Chapters	13

Chapter 2 Methodology	15
2.1 Methodology Overview	15
2.2 Study Architecture.....	16
2.3 Data Collection and Preprocessing	17
2.3.1 Data Collection Process:.....	18
2.3.2 Data Preprocessing	19
2.4 Feature Extraction and Analysis	20
2.4.1 ELA-based Feature Extraction:	21
2.5 Algorithm Selection and Development	22
2.5.1 CNN Development:	22
2.5.2 ELA Algorithm:.....	23
2.5.3 Noise Detection Algorithm:.....	23
2.5.4 Model Development:	23
2.5.5 Hardware and Software Setup:	24
2.6 Experimental Setup and Testing	24
2.6.1 Experimental Procedure:	24
2.6.2 Performance Metrics.....	24
2.6.3 Testing Results:	25
2.7 Used Tools and Technologies	25
2.8 Ethical and Legal Implications.....	26
2.9 Software Process Model.....	26
2.10 Research Requirements	27
2.10.1 Functional Requirements	27
2.10.2 Non-Functional Requirements.....	28
2.10.3 Software Requirement	28
2.10.4 Hardware Requirements	29
Chapter 3 Results and Discussion.....	30
3.1 Summary of the Experiments.....	30
3.1.1 Experimentation.....	30
3.1.2 Key results:	31
3.1.3 Analysis of Results	31
3.1.4 Real-Time Deployment	32
3.2 Results	33
3.2.1 ELA Covertng	33
3.2.2 Process of ELA Converting:.....	33

3.2.3 ELA and Noize Analysis	35
3.2.4 ELA Analysis	35
3.2.5 Check for Tampering:.....	36
3.2.6 CNN model Structure	36
3.2.7 Model Accuracy	40
3.2.8 Training and Validation Accuracy	41
3.2.9 Interpreting the Result	41
3.2.10 Impact of Preprocessing and Model Design.....	42
3.2.11 Interfaces	42
3.2.12 Outcomes	45
Chapter 4 Research Findings	47
4.1 Research Findings	47
4.2 Limitations and Challenges	49
4.3 Future Directions.....	51
4.4 Research Budget.....	53
Chapter 5 Research Timeline.....	54
Chapter 6 Conclusion.....	55
6.1 Conclusion.....	55
6.1.1 Summary of Major Findings.....	55
6.1.2 Contributions of the Research	56
6.1.3 Needs for study	57
6.1.4 Future Enhancements	58
6.1.5 Final Comments.....	59
References.....	60
Appendix 1: Research Publication	lxiv

List of Figures

Figure 2-1. Overall System Diagram	17
Figure 2-2. Dataset.....	18
Figure 3-1. Function to convert image to ELA format	33
Figure 3-2. ELA and Noize Analysis.....	35
Figure 3-3. CNN Model.....	38
Figure 3-4. CNN Model Architecture	39
Figure 3-5. Training Process of Model	40
Figure 3-6. Model Accuracy over Epochs	40
Figure 3-7. Loging Page	42
Figure 3-8. Sign Up Page.....	43
Figure 3-9. Main Page (Home)	43
Figure 3-10. History.....	43
Figure 3-11. About page 1	44
Figure 3-12. About Page 2.....	44
Figure 3-13. Logout	44
Figure 3-14. upload an Image.	45
Figure 3-15. Results (1)	45
Figure 3-16. Results (2)	46
Figure 6-1. Publication at scholar.google.com	lxiv
Figure 6-2. Paper page 1	lxv
Figure 6-3. Paper page 2	lxvi
Figure 6-4. Paper page 3	lxvii
Figure 6-5. Paper page 4	lxviii
Figure 6-6. Paper page 5	lxix
Figure 6-7. Paper page 6	lxx
Figure 6-8. Paper page 7	lxxi

List of Tables

Table 1-1. Research Gap.....12

Table 4-1. Research Budget.....53

Table 5-1. Research Timeline54