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is entirely my own and not of any other person, unless explicitly acknowledged (including citation of published and unpublished sources).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

List of Figures

List of Tables