INFORMATICS INSTITUTE OF TECHNOLOGY

INFORMATICS INSTITUTE OF TECHNOLOGY

In Collaboration with

UNIVERSITY OF WESTMINSTER

PureVisio: Explicit Content Blocking on the Client-side using a Hybrid Identification Model

A Dissertation by

Mr. Thomy Gevin De Croos

20191181 | w1790025

Supervised by

Mr. Obhasha Priyankara

Submitted in partial fulfilment of the requirements for the BSc (Hons) Computer Science degree at the University of Westminster.

May 2023

Abstract

The growth of pornography on the internet had created a significant challenge for parents and others worried about exposing their children to graphic sexual content. Porn detection algorithms were developed to identify and limit access to pornography websites and other sexually explicit internet material. However, these technologies had significant limitations and frequently failed to block explicit content or non-pornographic websites. Furthermore, porn detection software could be circumvented by accessing prohibited content using proxy servers, VPNs, or other means. As a result, a more effective and comprehensive strategy for identifying and blocking explicit information on the internet was required.

The goal of this research project was to create, construct, and test a hybrid identification model capable of identifying and blocking explicit material on the client side, with a primary focus on pornographic content as explicit content. By combining several elements of websites to identify and filter explicit material, the developed model addressed the limitations of existing detection systems. The model utilized a combination of image analysis and text analysis to accurately detect and block explicit content on the web, employing a CNN for image classification with an accuracy of 89.49% and an NLP LSTM model for text classification with an accuracy of 97.06%.

This research effort resulted in a complete hybrid identification model capable of properly detecting and blocking explicit content on the internet. This strategy assisted parents, schools, and internet service providers in safeguarding their children from inappropriate information. The findings of this study contributed to creating more effective measures for promoting internet safety and protecting individuals, particularly children, from the detrimental impacts of explicit information on the internet.

Keywords: Explicit Content Blocking, Convolutional Neural Networks (CNN), Natural Language Processing (NLP), Long Short-Term Memory network (LSTM).

Subject Descriptors:

- Computing methodologies → Artificial intelligence → Computer vision → Computer vision tasks → Visual Inspection
- Computing methodologies → Artificial intelligence → Natural Language Processing → Information Extraction