AN INTELLIGENT SYSTEM TO PREVENT THE SPREADING OF SENSITIVE CONTENT ONLINE

L. Jaba Sheela¹, S. Kousalya², R. Abinaya³

¹Professor, Department of Computer Science and Engineering, Panimalar Engineering College, Chennai, Tamil Nadu, India.
²Student, Department of Computer Science and Engineering, Panimalar Engineering College, Chennai, Tamil Nadu, India.
³Student, Department of Computer Science and Engineering, Panimalar Engineering College, Chennai, Tamil Nadu, India.

Email: ¹ljsheela@gmail.com, ²kousalya.s4798@gmail.com, ³abiresh1323@gmail.com

Corresponding Author: Dr. L. JabaSheela

https://doi.org/10.26782/jmcms.2020.05.00018

Abstract

In recent years, there is a striking surge in the availability of porn images and other such sensitive content on the Internet. Filtering of image porn has become one of the big challenges for searches; they are tied to finding methods to filter porn images and videos. Social media network is interested in filtering porn images from normal ones. The main objective of the proposed “Intelligent System to Prevent the Spreading of Sensitive Content Online” is to reduce the risk of harassment to a large extent by preventing anti-social elements from uploading such obscene content online. For attaining the ultimate goal, we will be using CNN algorithm to detect pornographic content. By RGB Channel Shifting, pixels of those pornographic contents will be corrupted in the device of the person trying to upload it on social media or internet. By using this “Intelligent System to Prevent the Spreading of Sensitive Content Online” we can prevent spreading of pornographic images/videos and thus avoid the harmful effects caused by these obscene practices.

Keywords: CNN algorithm, RGB channel shifting, pornographic content

I. Introduction

Over the past few years, technology has changed the way of communication of youth with their peers. According to recent survey, more than 75% of teenagers own cell phones, and one-third send over 3,000 text messages a month. In the last few years, new forms of electronic communication (e.g., Facebook, Twitter, Instagram, texting) have been created which are causing concern among health care professionals, parents, law enforcement and educators regarding the harmful practices...
that youth may engage in, as these types of communication are becoming more prevalent. Some of these harmful behaviors include cyber bullying, publicly posting obscene images, and communicating with or being solicited by prospective sexual predators online. Although there is no consistent legal definition for the term "sexting", most state laws generally concentrate on images and videos that are transmitted through cell phones. However, images and videos can also be distributed through computers, web cameras, or digital cameras. The broader definition of “sexting” given by Research studies is - “sending and/or receiving sexually suggestive images/videos or messages to peers through a cell phone to measure the prevalence of sexting behaviors among youth.”

In some social circles, sexting is an accepted occurrence that people consider a common practice. In other instances, it is a one-time lapse in judgment. Despite the reason for it, the number of teens using the built-in cameras on their iPads, smart phones and other electronic devices to take nude or sexually-suggestive pictures is rising exponentially. But what many of them do not realize is the unwelcomed consequences that come with along these choices.

Sexting has serious consequences not only for the person taking and sending the photos but also for the person receiving them. For example, most of the time sexting involves minors. So these nude photos are considered child pornography. As a result, sending or receiving of such messages is a crime.

Hence, we have proposed a system that can identify pornographic images before they are shared online and corrupt those images in the device. By this way of identifying the pornographic images, we can prevent the intrusion of such images into the internet. By corrupting the identified image, we can prevent the person from sharing that image by any means.

II. Literature Survey

Bei- Bei Liu et al [I] have proposed a novel two-stage scheme of pornographic image detection. Specifically, they first apply the content-based image retrieval technique to find out whether humans are present in the images. Then a detailed skin color analysis was performed to confirm the presence of pornographic content in the images.

Hong Zhu et al [II] have proposed a skin model based on the combination of YIQ, YUV, and HSV. In the pre-processing step, they have used white balance algorithm to achieve better skin area. Then, texture model based on Gray Level Co-Matrix and geometric structures of human beings were used to decrease the disruptions of the background region that were similar to the skin area. The features extracted from the last images dealt by color and texture model were given as input to the Support Vector Machines (SVM), through which the pornographic images and assorted control images were classified successfully.

I. Made Artha et al [III] have proposed that Convolutional Neural Networks can be applied to tackle the problem of pornographic image classification. In this research, a small modification to the last layer was proposed to fit the pornographic detection.
KaiLong Zhou et al [VI] have proposed a pornographic image recognition method based on convolutional neural network. This method can be classified into two sections—coarse detection and fine detection. Since majority of images are normal, they used coarse detecting to swiftly identify the normal images with no or fewer skin-color regions and facial images. For the images which contain very large amount of skin-color regions, they need further identification through fine detecting.

In the study made by Manuel.B.Garcia et al [VIII] an application was developed grounded from a pixel-based approach and a skin tone detection filter to identify images and videos with a large skin color count and they are considered to be pornographic in nature. With nudity detection algorithm being the base of the system, all the images and videos were subjected to preprocessing, segmentation, and filtration to analyze skin-colored pixels by processing them in YCrCrb space and then classifying them as skin or non-skin pixels.

MyoungBeom Chung et al [XI] have proposed an improved method that first utilizes Canny Edge to analyze the fine grains of the image to determine if the image is of high quality or low quality, and then to determine whether the image passes the final obscenity test. To check the efficacy of this method, a randomly selected set of images was first subjected to the Canny Edge test, to separate the batch into two groups based on the image-quality level. The images were then checked for their obscenity levels twice, first with the existing method and then with the method that was proposed in this paper.

Yuan Xu et al [XIV] have published a paper in which a framework for pornographic image detection based on skin region information has been proposed. Different from traditional works, their approach extracts color and texture features from arbitrary-shaped segmented regions. Then Gaussian Mixture Models were built for skin and non-skin region classification, and the skin map was produced based on the classification result. Finally, features of the Eigen region were used to describe the layout of skin regions on the whole image and pornographic images were detected according to the skin modality.

WaheerYaqub et al [XV] have proposed a system in which a pornographic image is encrypted using order preserving encryption, randomization, and permutation. In this system, skin pixels were detected from the encrypted image in the encrypted domain without revealing the image content. The proposed scheme is shown to have low overhead and no degradation in detection accuracy from various experiments and analysis that were conducted.

III. System Architecture

Classification Module

This module does the image classification and detects whether the image has pornographic content or not. For this we use a deep convolutional neural network model to classify the images and detect pornographic content. This module can also analyze video clips that are being uploaded. The video clips are divided into several frames and each frame is analyzed the same way, an image is analyzed. This model is trained using several training datasets until expected accuracy is achieved.
Corruption Module

After analyzing the image, if it is found to possess sensitive content, then it is corrupted in the device from which it is being uploaded. This is done by RGB Channel Shifting the pixels of the image under analysis and then bit shifting them. Channel shifting is the process in which the red, green or blue values of pixels in an image are taken and those values are applied to pixels in different positions on the image. By this way we can prevent the person from uploading or sharing the pornographic image in any kind of social media platforms.

Fig. 1: System Architecture

Fig. 2: RGB Channel Shifting
IV. Methodology

While scanning the media to be uploaded, the proposed software will automatically detect the images and video files with pornographic content, and will disable the spreading of those sensitive content by corrupting that particular media file in the device. By this way we can prevent spreading of pornographic images/videos and thus avoid the harmful effects caused by these practices.

All the above mentioned objectives are achieved by providing the proposed system as a plug in service to various social media platforms people commonly use as a means of sharing images and videos.

V. Results

From the experimental results we can infer that the performance of the system on training and testing dataset is almost the same. This proposed system performs with a 97.2% recall precision and 2.8% false positive rate on the testing dataset.

The results after comparing the proposed system with several other systems are shown in Table I.
Table 3: A Comparison with Other Systems

| S.No. | Algorithm/System                                                                 | Recall Precision (%) | False Positives (%) |
|-------|----------------------------------------------------------------------------------|----------------------|---------------------|
| 1     | Obscene Image Detection Algorithm [XI]                                            | 83.2                 | 16.8                |
| 2     | A Pornographic Image and Video Filtering Application Using Optimized Nudity Recognition and Detection Algorithm [VIII] | 89.01                | 10.99               |
| 3     | Convolution Neural Network for Pornographic Images Classification [III]            | 93.8                 | 6.2                 |
| 4     | An Intelligent System to Prevent the Spreading of Sensitive Content Online        | 97.2                 | 2.8                 |

Figure 4 shows the graph that has been generated by plotting the accuracy against epoch.

VI. Conclusion

The proposed system can thus prevent uploading of obscene pornographic content online. It can also help cyber forensic department to identify the cybercriminals. By adapting this system in every common social media platforms, the dignity and modesty of the victims and common people can be protected online. But still, it is important for parents to talk with their kids and teen children about the consequences of these illegal practices. Apart from creating awareness among the teens about the emotional consequences of sexting, they also need to know about the legal repercussions as well.
References

I. B. Liu, J. Su, Z. Lu and Z. Li, "Pornographic Images Detection Based on CBIR and Skin Analysis," 2008 Fourth International Conference on Semantics, Knowledge and Grid, Beijing, 2008, pp. 487-488. doi: 10.1109/SKG.2008.48

II. H. Zhu, S. Zhou, J. Wang and Z. Yin, "An algorithm of pornographic image detection," Fourth International Conference on Image and Graphics (ICIG 2007), Sichuan, 2007, pp. 801-804. doi: 10.1109/ICIG.2007.29

III. I. M. A. Agastya, A. Setyanto, Kusrini and D. O. D. Handayani, "Convolutional Neural Network for Pornographic Images Classification," 2018 Fourth International Conference on Advances in Computing, Communication & Automation (ICACCA), Subang Jaya, Malaysia, 2018, pp. 1-5. doi: 10.1109/ICACCAF.2018.8776843

IV. Islam, MdKamrul, MdManjur Ahmed, and Kamal ZuhairiZamli. "Identifying the Pornographic Video on YouTube Using Vlog Stream." 2018 4th International Conference on Computing Communication and Automation (ICCCA). IEEE, 2018.

V. J. Shayan, S. M. Abdullah and S. Karamizadeh, "An overview of objectionable image detection," 2015 International Symposium on Technology Management and Emerging Technologies (ISTMET), Langkawi Island, 2015, pp. 396-400. doi: 10.1109/ISTMET.2015.7359066

VI. K. Zhou, L. Zhuo, Z. Geng, J. Zhang and X. G. Li, "Convolutional Neural Networks Based Pornographic Image Classification," 2016 IEEE Second International Conference on Multimedia Big Data (BigMM), Taipei, 2016, pp. 206-209. doi: 10.1109/BigMM.2016.29

VII. L. Lv, C. Zhao, H. Lv, J. Shang, Y. Yang and J. Wang, "Pornographic images detection using High-Level Semantic features," 2011 Seventh International Conference on Natural Computation, Shanghai, 2011, pp. 1015-1018. doi: 10.1109/ICNC.2011.6022151

VIII. M. B. Garcia, T. F. Revano, B. G. M. Habal, J. O. Contreras and J. B. R. Enriquez, "A Pornographic Image and Video Filtering Application Using Optimized Nudity Recognition and Detection Algorithm," 2018 IEEE 10th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment and Management (HNICEM), Baguio City, Philippines, 2018, pp. 1-5. doi: 10.1109/HNICEM.2018.8666227

IX. Moreira, Danilo&Fechine, Joseana. (2018). “A Machine Learning-based Forensic Discriminator of Pornographic and Bikini Images.” 1-8. 10.1109/IJCNN.2018.8489100.
X. Murugavalli, S., et al. "Enhancing security against hard AI problems in user authentication using CAPTCHA as graphical passwords." International Journal of Advanced Computer Research 6.24 (2016): 93.

XI. MyoungBeom Chung, IlJuKo and DaeSik Jang, "Obscene image detection algorithm using high-and low-quality images," 4th International Conference on New Trends in Information Science and Service Science, Gyeongju, 2010, pp. 522-527.

XII. Sheela, L. Jaba, V. Shanthi, and D. Jeba Singh. "Image mining using association rules derived from feature matrix." Proceedings of the International Conference on Advances in Computing, Communication and Control. 2009.

XIII. Thenkalvi,B., and S. Murugavalli, “Image retrieval using certain block based difference of inverse probability and certain block based variation of local correlation coefficients integrated with wavelet moments." Journal of Computer Science 10.8 (2014): 1497.

XIV. Y. Xu, B. Li, X. Xue and H. Lu, "Region-based Pornographic Image Detection," 2005 IEEE 7th Workshop on Multimedia Signal Processing, Shanghai, 2005, pp. 1-4. doi: 10.1109/MMSP.2005.248675

XV. Yaqub, Waheeb&Mohanty, Manoranjan&Memon, Nasir. (2018). “Encrypted Domain Skin Tone Detection For Pornographic Image Filtering”. 1-5. 10.1109/AVSS.2018.8639350.

XVI. Zhang, J., Sui, L., Zhuo, L., & Li, Z. (2013). “Pornographic image region detection based on visual attention model in compressed domain”. IET Image Processing, 7, 384-391.