6th International Conference on Multidisciplinary Research (ICMR-2019)
Osmania University Campus, Hyderabad (India)
30th-31st May 2019 www.conferenceworld.in
Conference World
ISBN : 978-93-87793-89-7

ANALYSIS OF DIGITAL IMAGE PROCESSING TECHNIQUES AND FILTERING TOOLS: CYBER AWARENESS FOR WOMEN AND CHILDREN

Dr. Shantha Visalakshi. U[1]

[1](*Assistant Professor, MCA Department, Ethiraj College for Women (Autonomous), TN, India)*

ABSTRACT

In recent days, the advent of Information and Communication technology has grown enormously and the benefits obtained from Cyber technology has taken almost all the business models into greater heights. With the same intense cyber crime has also got increased equally and the protection against all sought of threats in cyber space are essential. As it is not only necessary to incorporate some of the basic awareness over cyber access and availing its services online, but also to learn about some of the possible digital image processing techniques to integrate cyber awareness by means of avoiding risks. In this paper both general and technical cyber awareness tips and safe search engineering techniques are going to be analyzed; thereby, the ultimate scapegoats of cyber space can be safeguarded and the cyber access with lesser risks is ensured.

Key words: Cyber Crime, Cyber Awareness, Digital Image Processing, Information and Communication Technology.

INTRODUCTION

Cyber crimes against women and children are kept on increasing and they have been significantly persecuted in the cyberspace. Some people try to defame women and children by sending harassment e-mails, stalking women and children by using chat rooms, websites and other possible cyber space, creating pornographic videos where women and children are portrayed in an unfair way without their knowledge and assent, spoofing e-mails, morphing of images for pornographic content, trolling, phishing etc., Intensive cyber awareness needs to be catered among women and children regarding the safe use of Mobile Phones, Computers and all possible devices accessed over the Internet. Those who emphasize the importance of online security generally contradict themselves through their actions and as a result are likely to fall victim to cybercrime [1].

REVIEW OF RELATED WORK

The cyberspace has been a boon to the human civilization as Internet has connected people around the globe. The desire to know what is unknown is indispensable of human nature has aggravated the urge of discovering the untraded path which led to the unearthing of the cyber world [2]. To spot the major cause for the cyber crime against women is that the transcendental jurisdiction of Internet. [3]. A hybrid method of rule-based

processing and back-propagation neural networks for spam filtering proved to be much more robust compared to other spam detection techniques [4]. Google Cloud vision API offers image analysis as a service with safe search detection algorithm that determines image safe search properties on the image i.e., the likelihood of the image might contain violence or nudity. The Social Networking websites have developed a new arena for socializing. From online shopping to net banking, from e-ticketing to e-tax filing it has made the life of women easy [5]. Predictable acumen guides us to consider that women are more emotionally expressive than men are. [6]. Many of the legal support has been initiated to mitigate the cyber crime. Agencies dealing with cases of cyber violence need to have a high degree of technical competency. They need to be well formed about the legal provisions [7].

CYBER-SAFE ARCHITECTURE

To access the cyber even safer, many of the technical tools and legal assistance are available in the real time. Among the available filtering techniques some of them can be mounted prior to the cyber access and some may be posterior. It is always advisable to avoid the consequences by being cautious towards our each and every moves over cyber space. Accordingly, the prior filtering techniques suggested are RSOR algorithm [8] which concentrates on nudity detection and elimination, Safe search detection [10] which concentrates on finding inappropriate contents and Internet filtering programs [9] concentrate on the complete monitoring over the cyber access. And the posterior filtering technique suggested is Reverse Image Processing [11] which purely concentrates on finding the related image for the image input query supplied.

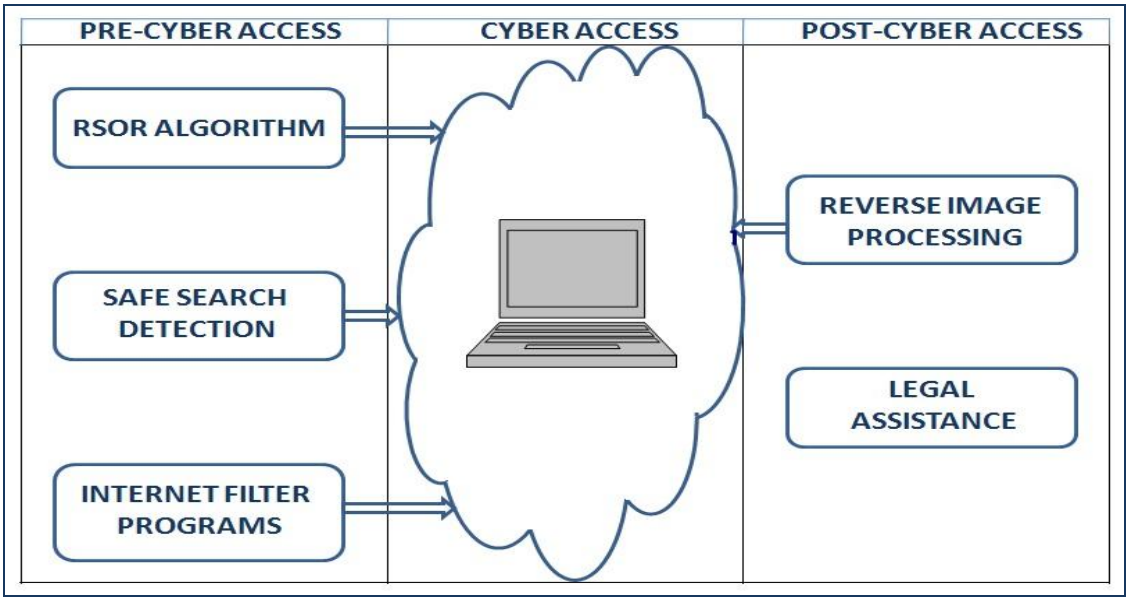

Fig 3.1: Cyber Safe Access Techniques and Tools

In addition to the prior and posterior technical tools much more legal laws were defined under Information Technology Act 2000 and passed on against the cyber predators. Legal laws can be passed on against the cyber crime like Defaming of a person's identity, Cheating, and Violation of privacy, Stalking and Publishing obscene material in an electronic medium etc., As the tools and techniques are the boon to the cyber safe access, it's worth enough to deal about each and every techniques in a detailed manner as follows.

FILTERING TECHNIQUES

RSOR Algorithm: The algorithm has been implemented based on the recognition and selection of image regions as well as the performing of operations on the regions found with the digital images in order to detect nudity. The pixel segmentation comprises HSV color model used to find and omit the pixels corresponding to the human skin is used. The RSOR algorithm (Recognition, Selection and Operations in Regions) has been implemented to recognize, and to separate the image region with the highest number of skin pixels within the segmented image.

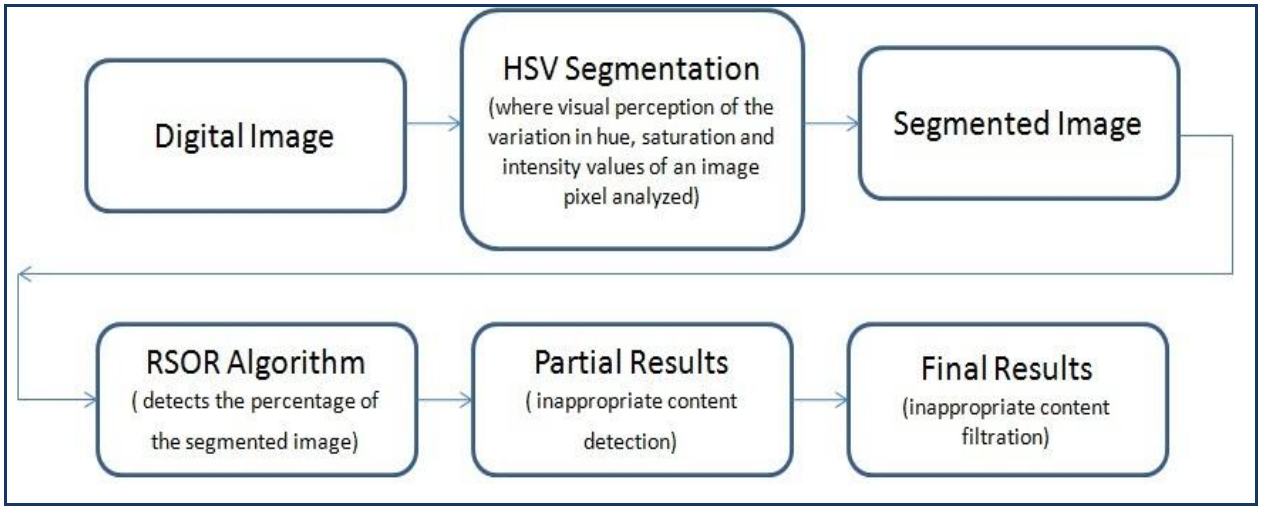

Fig 3.2: RSOR Algorithm Functionality

The algorithm utilizes the combination of HSV Segmentation and RSOR algorithm to track and detect inappropriate content on the cyber space thereby filtering of such contents can be removed off subsequently. The DigImFilt (client) and DigImFilt Services (Server) web services developed by Microsoft offering the finest filtration of inappropriate content [Gullen 2016].

SAFE_SEARCH_DETECTION: The Cloud Vision API safe search detection feature uses a deep neural network model specially trained to classify inappropriate content in images. The safe search engineering team has built a debug tool to analyze the image classifications and better understand the deep neural networks powering the detection model. Using the internal neural network activations and back propagation gradients,

ISBN : 978-93-87793-89-7

this tool imposes a heap map on the image indicating the parts that the classifier identified as possibly explicit. The spoof detection classifier primarily looks for memes which are indicated by the presence of text, typical meme faces and backgrounds. The Adult content classifier is trained to separate pornographic and non-pornographic images. This classifier programmed in such a way not to flag pictures that contain nudity in a medical, scientific, educational or artistic content. Rather than reviewing all content manually, the Vision API lets you to automate the content approval process and significantly reduces the number of images requiring manual review.

INTERNET FILTER PROGRAMS: In addition to the algorithms and various other techniques for a safe search facility over Internet, there are quite good number of Internet Filter application paid programs is available. They are:

Qustodio: Qustodia works on both computers and smart devices and it has 29 filter categories and useful time controls. The detailed reports include screenshots of the websites can be generated for the concerned parents. It offers 'Smart' filters such as Social monitoring, Access controls, app monitoring, Location tracking, Calls & text messages monitoring and blocking, Multiple Users and Devices, Web based dash board, Activity reports, Danger Alerts, Panic Alerts and Parental app.

Net Nanny: Net Nanny is an inexpensive Internet filter program includes 18 filter categories and profanity masking that covers foul language on websites and blocks them from being typed into messages. Screen Management and Remote access are the features added. With this program it is ensured that digital habits can be monitored and safe-guarded from harmful content.

Surfie: Surfie has both a desktop and mobile app so the absolute monitoring over cyber activities is assured. It has got 18 specialized filters like blocking websites, setting time limits and capturing messages. Also it provides anti-cyberbullying and stalking features.

SpyAgent: SpyAgent provides an unrivaled set of essential computer monitoring features as well as website and application content filtering, chat client blocking, real-time activity alerts and remote delivery of logs via email or FTP.

Verity: Verity is an effective website blocker that can ban specific sites from being accessed by certain users. The features wrapped off with Verity are: Keystroke recording, screenshot capture, Reporting and Notification and Time Management feature.

REVERSE IMAGE PROCESSING

Reverse image search is a search engine technology that takes an image file as input query and returns results related to the image. Search engines offer reverse image capability includes Google and TinEye. Reverse

Image capability offers: Locating the source information of an image, searching for duplicated content, Ensuring compliance with copyright regulations, Finding information about unidentified products and other pertinent objects, Debunking fake images and Finding higher resolution versions of images. The practical uses may get extended such as Find an apartment, Find names of unlabeled products, Find recipes from images, Figure out celebrity names, Debunk social media posts and profiles, Track down wall papers and High resolution originals, Find your own artwork is being used, Track down original artists, Identify plants, animals and more.

From all of the above techniques, it is clearer that the cyber safe access can be gained by incorporating both priori and posterior techniques. Thereby it is ensured that the most common cyber crime activities like publishing inappropriate contents, Stalking and Violation of Privacy etc., can be mitigated by means of these filtering algorithms and programs.

LEGAL SUPPORT & GUIDANCE

Several sections of breaching of privacy have been defined under Information and Technology Act 2000 include are listed in Table 4.1. As many of the laws were defined against the cyber crime predators were developed, the cyber victim also should come out in punishing them so as to reduce the same.

Table 4.1: Legal Assistance for Cyber Safe Access

Section 67	:	Punishment for publishing or transmitting obscene material in electronic form. (Whoever publishes and transmits)
Section 66A	:	Punishment for sending offensive messages through communication service etc.,
Section 66B	:	Whoever dishonestly receives or retains any stolen computer resource shall be punished.
Section 66C	:	Punishment for identity theft whoever, fraudulently or dishonestly make use of electronic signature, Password and other unique identification feature of any other person.
Section 66D	:	Punishment for cheating by personation.
Section 66E	:	Punishment for violation of privacy.
Section 66F	:	Punishment for cyber terrorism.
Section 72	:	Penalty for breach of confidentiality and privacy.
Section 72A	:	Punishment for disclosing information during lawful contract.

Section 441 IPC	:	Deals with criminal trespassing.
Section 354D	:	Deals with Stalking.

Even though many of the laws were defined against cyber crime, they were not defined for the avoidance of crime against women and children. To mitigate and thwart cyber crime against women i.e., to prevent their modesty being outraged in cyber space, some more amendments need to come up in the present statutes.

CONCLUSION

Being the net users, women and children in specific should not share any of their personal identity related information. Within the cyber space it is expected to have each and every move in a measured manner. It is the bounded duty of the users to be even more careful in adding names in their friends list. Also, the service providers like any messaging app and social media networks should ensure the adequate access mechanisms over the appropriate contents uploaded. The lesser the accessibility over the contents is greater the safe behind the screen. Hence, the filtering programs and the techniques are the real boon mechanisms to have the cyber safe access. In spite of having all these precautionary measures, the defamer or the abuser must think about the consequences before committing any offence. Immediate reporting to the cyber wing of police would obviously help in capturing the offenders. Though, much more laws were defined under IT Act-2000, even more strict punishments and actions which are immediate and effective to be taken.

REFERENCES

[1] Symantec, Norton Cyber Security Insights Report, 2017.

[2] Keyun Ruan, Cyber crime and Cloud Forensics: Application for Investigation Processes, ISBN: 978-1-4666-2693- 5, 2013.

[3] Shobana Jeet, Criminal Law: Cyber crimes against women in India: Information Technology Act, 2000, ISSN: 2229-712X, Jun 2012 Pg: 8891-8895.

[4] Ching Wu et al., Behavior based spam detection using a hybrid method of rule based techniques and neural networks, International Journal of Expert systems with Applications, ISSN No: 0957 – 4174, Vol 36 No 3 Apr 2009 Pg: 4321-4330.

[5] Debarati Halder and Jaishankar. K, Cyber socializing and victimization of women, TEMIDA, ISSN: 1450-6637, Sep 2009 Pg: 5-26.

[6] Roisin Parkins, Gender and Emotional Expressiveness: An Analysis of Prosodic Features in Emotional Expression, Griffith Working Papers in Pragmatics and Intercultural Communication Vol 5 No 1, 2012 Pg: 46-54.

ISBN : 978-93-87793-89-7

[7] Megha Biji Joseph et al., Cyber Violence- Unpacking Case Histories from Counselling Centres, Cyber Crime Cells, The National University of Advanced Legal Studies, Kochi, Pg: 1-8.

[8] Luis Enrique et al., Approach of RSOR Algorithm using HSV Color Model for Nude Detection in Digital Images, Computer and Information Sciences, ISSN: 1319-1578, Vol 4 No 4, Jul 2011 Pg: 29-45.

[9] https://www.toptenreviews.com/software/security/best-internet-filter-software/

[10] https://cloud.google.com/blog/products/gcp/filtering-inappropriate-content-with-the-cloud-vision-api

[11] Zhengxi Wei et al., Design and Implementation of image search algorithm, American Journal of Software Engineering and Applications, ISSN: 2327-2473 Vol 3 No 6 Dec 2014 Pg: 90-94.

[12] Dr. Monika Jain, Victimization of Women beneath cyberspace in Indian upbringing, Bharathi Law Review, Jun 2017 Pg: 1-11

[13] Shweta Sankhwar et al., Woman Harassment in Digital Space in India, International Journal of Pure and Applied Mathematics, ISSN: 1314-3395 Vol 118 No 20, 2018, Pg: 595-607.

[14] Selma Dilek et al., Application of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review, International Journal of Artificial Intelligence and Applications, ISSN: 1560-4306, Vol 6 No 1, Jan 2015, Pg: 21-39.

[15] Tanaya Saha et al., Indian Women at Risk in the Cyber Space: A Conceptual Model of Reasons of Victimization, International Journal of Cyber Criminology, ISSN: 0974-2891, Vol 8 No ,1 Jan 2014, Pg: 57-67.